



The bridge to possible

Firewall Threat Defense (FMC 管理) Version 7.0 初期セットアップガイド Vol. 3 応用設定編 Rev 2.0

August 2022

シスコシステムズ合同会社

はじめに

- 本ガイドは、Version 7.0 の Firewall Management Center (以下、FMC) 管理の Firewall Threat Defense (以下、FTD) の初期セットアップ方法を解説しております。
- 本ガイドは、FTD と FMC の仮想版を使って、評価作業を開始できることをゴールとしております。
- 本ガイドは、4部作の Vol. 3 に相当します。

内容に関する保証について

- 本ガイドは、2022年8月現在の情報に基づいており、FTD & FMC のソフトウェアは 7.0.x を、ハイパーバイザは VMware ESXi 6.5 を利用しております。
- 本ガイドに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。
- シスコは、本ガイドに関して、その正確性又は完全性について一切の責任を負わないこととします。
- シスコは、本ガイドが十分な品質を有すること、特定の目的に対する適合性を有すること、又は第三者の知的財産権、プライバシー権等その他の一切の権利に対する侵害がないことを、明示にも黙示にも表明又は保証しません。

ネットワーク環境図

Internet

■ 設定済みの機器

MGMT NW

.135.254

DNS: 64.104.14.184

ntp.esl.cisco.com

proxy-wsa.esl.cisco.com

10.71.128.0/21

VM Network

.132.194

G0/0 outside .1

FTDv01

test PC2

Management

G0/1 inside .1

.101

.132.204

FMCv

.132.130

ISE-PIC01

.132.220

ESXi

.132.131

AD01.secvt.jp

内部LAN
192.168.1.0/24

.11

test PC1

g0/0 グローバルアドレス

ASA

g0/3 .254

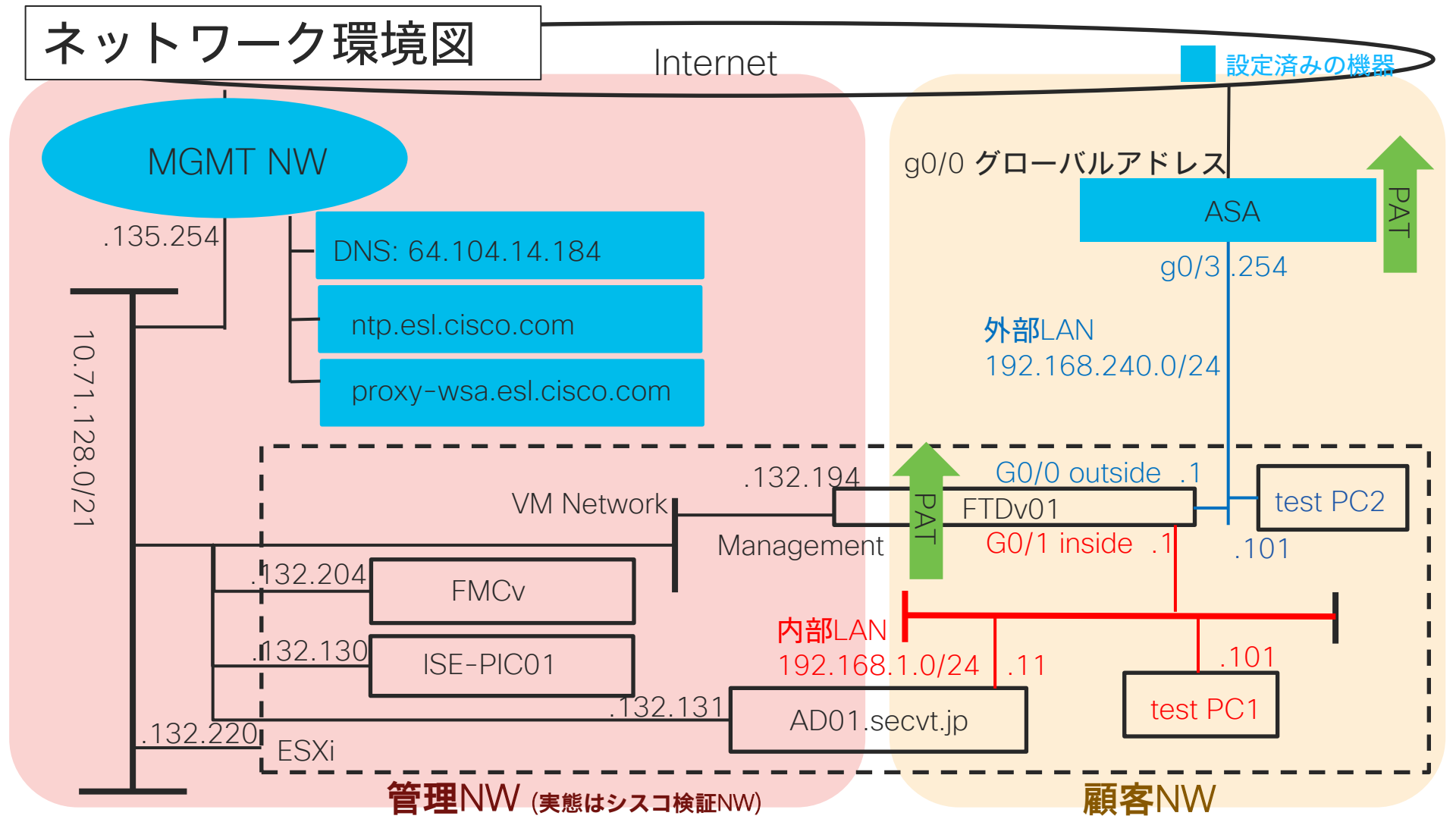
外部LAN

192.168.240.0/24

PAT

管理NW (実態はシスコ検証NW)

顧客NW



当ガイド (Vol. 3) のシナリオ

- SSL Policy にて内部から外部への通信を復号し、セキュリティ検査を適用する。
- ISE-PIC を導入し、Active Directory と連携することで、AD ログオン時のユーザによってセキュリティポリシーを使い分ける Identity Firewall を利用する。
- FTDv にて AnyConnect を使ったリモートアクセス VPN を接続を提供し、さらに VPN 接続時にもセキュリティポリシーを適用する。
- FTDv, FMCv のバックアップを取得し、有事の際のリストアを検証する。

注意事項

- 製品名称が更新されているが、ソフトウェア名称は旧製品のままで公開されている
- 新名称 ↔ 旧名称
 - Firewall Management Center ↔ Firepower Management Center
 - Firewall Threat Defense ↔ Firepower Threat Defense

Vol.1 (初期インストール編) の目次

1. FMC と FTD のインストール
 - 1-1. FMCv の初期インストール
 - 1-2. FTDv の初期インストール
 - 1-3. (Option) FPR4100/9300 シリーズの初期インストール
 - 1-4. (Option) FPR1000/2100 シリーズの初期インストール
2. FTD と FMC その他初期設定
3. シグネチャ及び各種 DB の更新
4. スマートライセンスの適用
5. FMC と FTD の Upgrade / Patch インストール

Vol. 2 (基本セキュリティポリシー設定編) の目次

6. Routed Firewall, NAT および Network Discovery の設定
7. Prefilter の設定
8. Intrusion Policy の設定 (Snort3)
9. Malware & File Policy の設定
10. Access Control Policy の設定

Vol. 3 (応用設定編:当ガイド) の目次

11. TLS Decryptionの設定
12. IDFW の設定
13. AnyConnect VPN 接続の設定
14. バックアップの設定とリストアの方法

Vol. 4 (管理・監視・冗長構成編) の目次

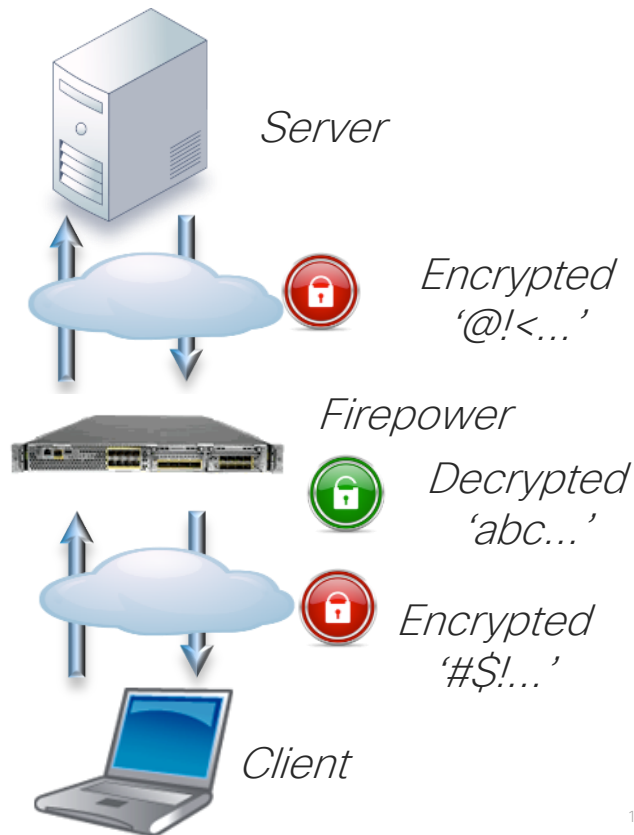
- 15. FMC API の利用例
- 16. システム監視
- 17. Syslog・レポート・アラートの設定
- 18. SAL SaaS, SecureX 連携の設定
- 19. 設定ロールバック
- 20. FTD High Availability の設定
- 21. FMC High Availability の設定

11. TLS Decryption の設定

TLS 復号アクセラレーション

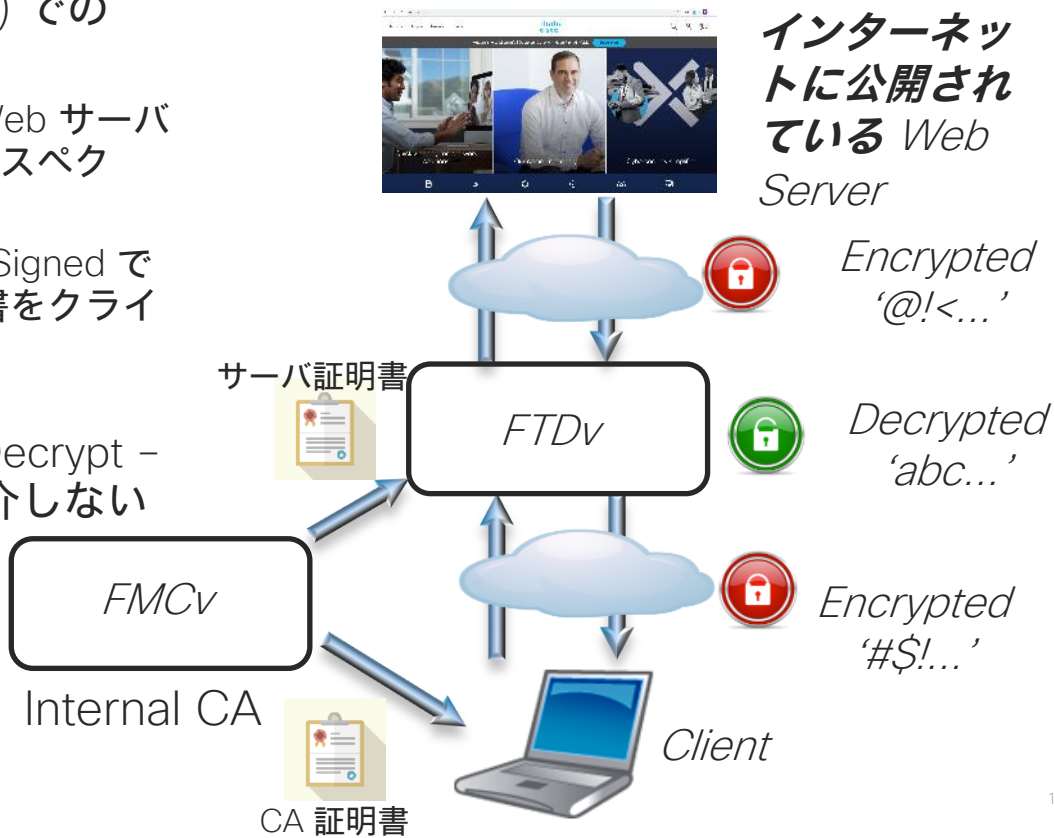
- SSL/TLS 暗号通信を復号してインスペクションを行う機能
- inbound inline (L1), transparent (L2), routed (L3)
 - Decrypt - Known Key 設定を利用
 - 主に不特定多数の端末から自身が管理している公開サーバへの通信を復号。IPS 機能と併用される場合が多い
- outbound inline (L1), transparent (L2), routed (L3)
 - Decrypt - Resign 設定を利用
 - 主に自身が管理しているネットワーク内から不特定多数の公開サーバへの通信を復号。NGFW 機能と併用される場合が多い
- Firepower 1K,3K,4k,9k はハードウェア処理による高速処理が可能。詳しくはデータシート参照
- 復号・再暗号化や仲介管理が、負荷や遅延の原因となるため、必要な通信のみ Decrypt するなどメリハリ付けを
(運用例：定期バックアップや信頼サイトは Decrypt しない)
- Inline TAP, passive interface では未サポート

FTD は MITM (Man In The Middle) の形で通信を復号し、インスペクション後にまた通信を暗号化する



このガイドでのシナリオ

- Outbound (i.e. Decrypt - Resign) での TLS 復号をを紹介
- インターネットに公開されている Web サーバにアクセスする際に、FTD でのインスペクションを行う
- 簡素化のため、Internal CA を Self-Signed で FMC にて立ち上げ、その CA 証明書をクライアントにインストールする
- このガイドでは、Inbound (i.e. Decrypt - Known Key) での TLS 復号は紹介しない



ステップ1: FMC での Internal CA 作成

FMC
Object Management

Overview Analysis Policies Devices Objects AMP Intelligence Deploy

Internal CAs

Generate CA Internal CA Filter

Generate Internal Certificate Authority

Name

Name: FMC-CA

Country Name (two-letter code): JP

State or Province: Tokyo

Locality or City: Minato-ku

Organization: CiscoSystemsGK

Organizational Unit (Department): CISCO-JP

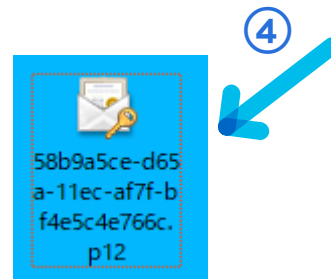
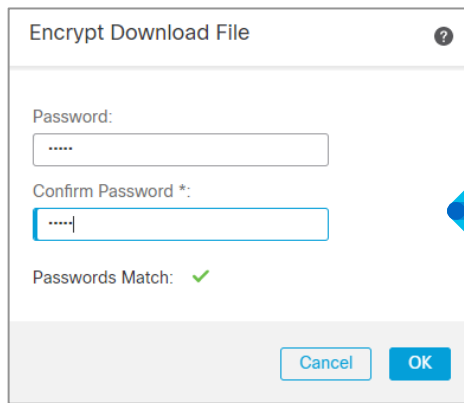
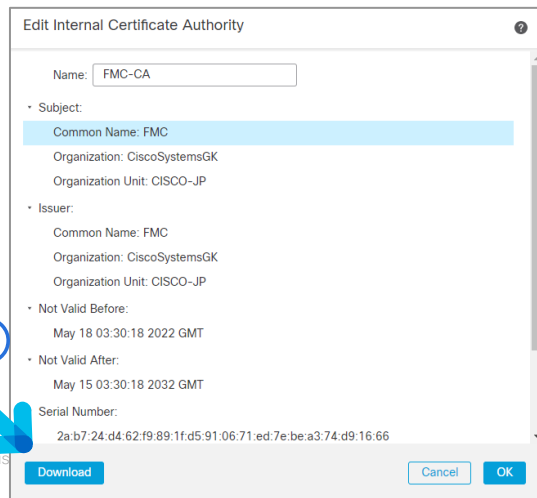
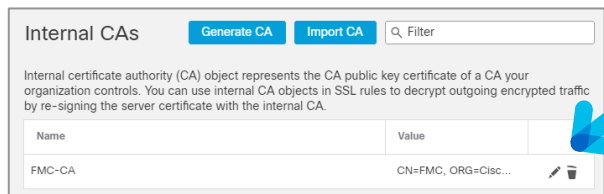
Common Name: FMC

Generate CSR Cancel Generate self-signed CA

- ① FMC にて Objects > Object Management を選択
- ② PKI > Internal CAs を選択
- ③ Generate CA をクリック
- ④ Internal CA に必要なパラメータを埋める
- ⑤ Generate self-signed CA をクリック
- ⑥ Internal CA が作成される

ステップ2-1: Internal CA の証明書を入手

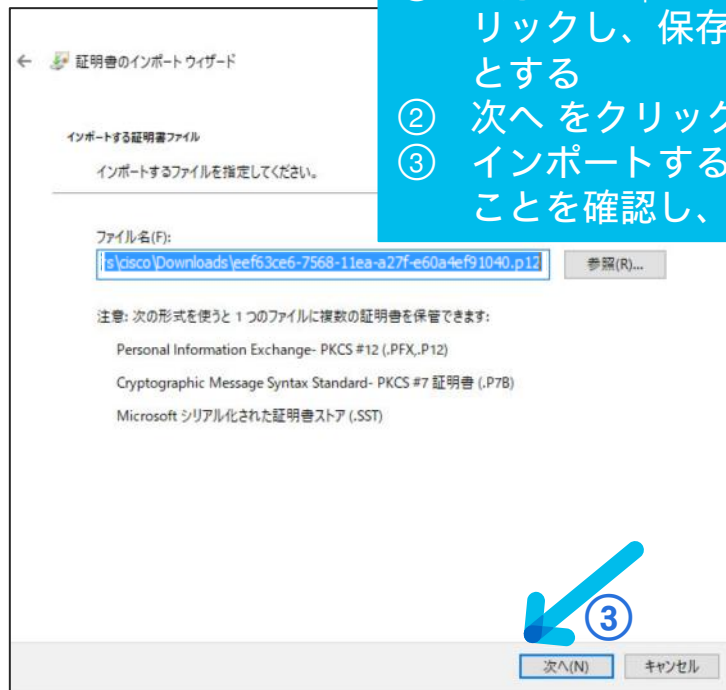
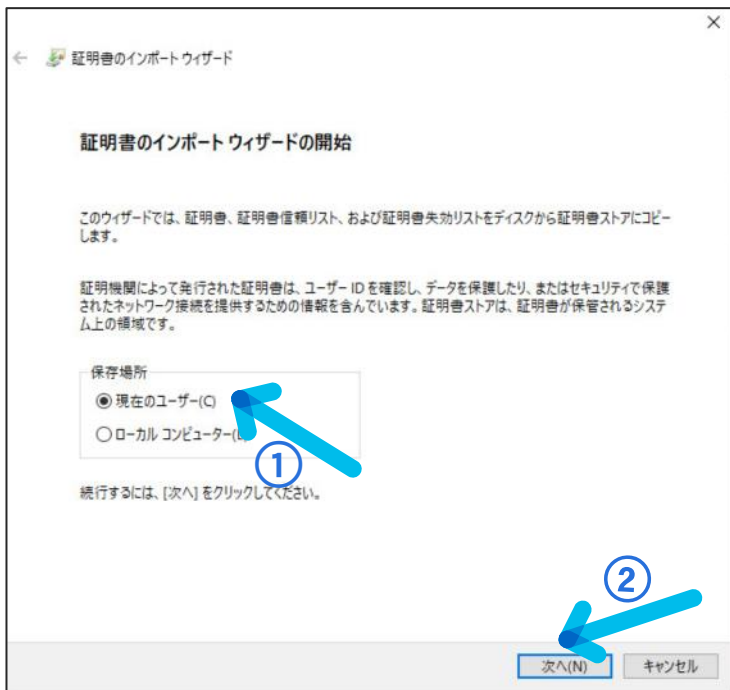
テスト PC は FMC の Internal CA を信頼する必要があるため、Internal CA の証明書をテスト PC の「信頼されたルート証明機関」にインポートする。まずは Internal CA の PKCS #12 形式のファイルを手にする



- ① 作成した Internal CA の Edit (鉛筆アイコン) をクリック
- ② Download をクリック
- ③ PKCS #12 ファイルの任意パスワードを設定した後、OKをクリック
- ④ PKCS #12 ファイルが自動ダウンロードされる

ステップ2-2: PC への Internal CA 証明書のインポート(参考)

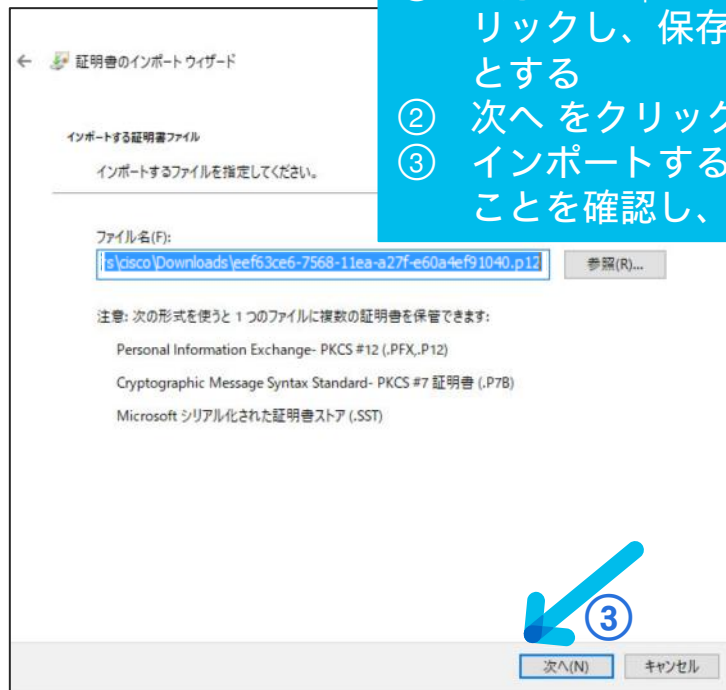
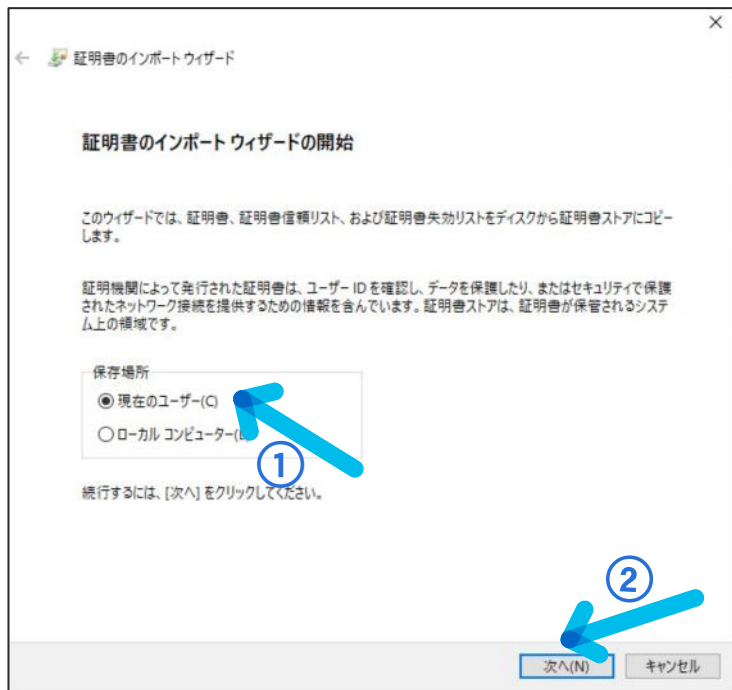
入手した Internal CA の PKCS #12 形式のファイルを、テスト PC にコピーし、インポートする。ここでは Windows 10 でのインポート手順を参考として記載



- ① 入手した .p12 ファイルをダブルクリックし、保存場所を現在のユーザーとする
- ② 次へ をクリック
- ③ インポートするファイルが合っていることを確認し、次へ をクリック

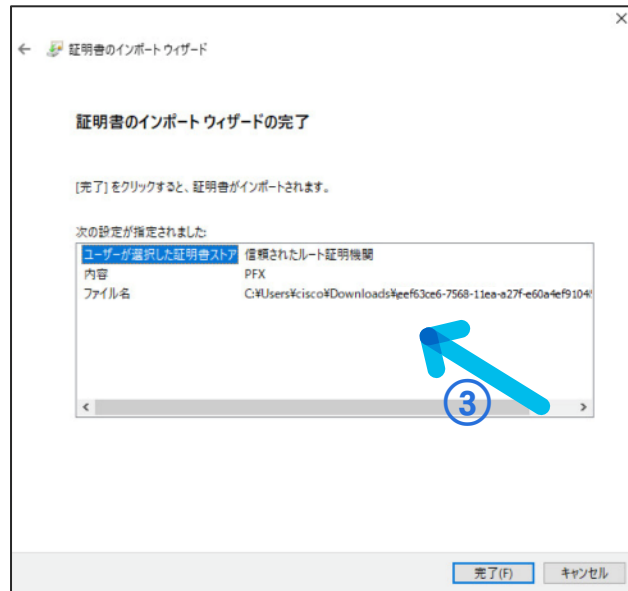
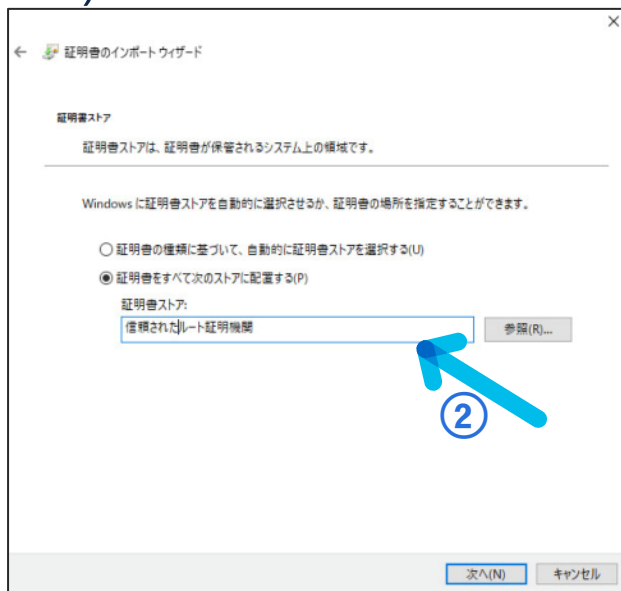
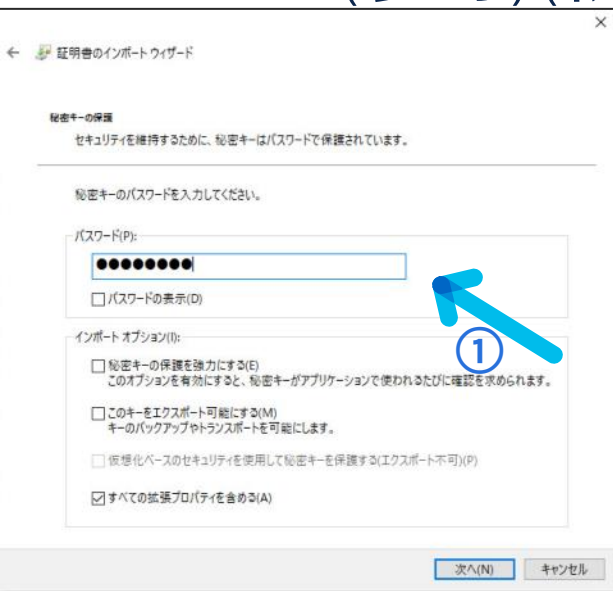
ステップ2-2: PC への Internal CA 証明書のインポート(参考)(続き)

入手した Internal CA の PKCS #12 形式のファイルを、テスト PC にコピーし、インポートする。ここでは Windows 10 でのインポート手順を参考として記載



- ① 入手した .p12 ファイルをダブルクリックし、保存場所を現在のユーザーとする
- ② 次へ をクリック
- ③ インポートするファイルが合っていることを確認し、次へ をクリック

ステップ2-2: PC への Internal CA 証明書のインポート(参考)(続き)



- ① FMC で設定した PKCS #12 のパスワードを入力し、次へ をクリック
- ② マニュアルで証明書ストアに「信頼されたルート証明機関」を選択し、次へ をクリック
- ③ ファイル名や証明書ストアが正しいことを確認し、次へ をクリック

ステップ2-2: PC への Internal CA 証明書のインポート(参考)(続き)



発行先	発行者	有効期限	目的	フレンドリ名	操作
Baltimore CyberTrust Root	Baltimore CyberTrust Root	2025/05/13	クライアント認証, コ...	DigiCert Baltimore ...	証明書 ▲
Buypass Class 2 Root CA	Buypass Class 2 Root CA	2040/10/26	クライアント認証, 暗...	Buypass Class 2 Ro...	他の... ▶
Certum CA	Certum CA	2027/06/11	クライアント認証, コ...	Certum	FMC ▲
Certum Trusted Network CA	Certum Trusted Network CA	2029/12/31	クライアント認証, コ...	Certum Trusted Net...	他の... ▶
CFCA EV ROOT	CFCA EV ROOT	2029/12/31	クライアント認証, コ...	CFCA EV ROOT	
Cisco Root CA M1	Cisco Root CA M1	2033/11/19	<すべて>	<なし>	
Cisco Systems, Inc.	DigiCert Trusted G4 Code Signing ...	2023/09/28	コード署名	<なし>	
Cisco Umbrella Root CA	Cisco Umbrella Root CA	2036/06/29	<すべて>	<なし>	
Class 3 Public Primary Certificati...	Class 3 Public Primary Certificatio...	2028/08/02	クライアント認証, コ...	VeriSign Class 3 Pub	
COMODO RSA Certification Aut...	COMODO RSA Certification Auth...	2038/01/19	クライアント認証, コ...	Sectigo (formerly C...	
Copyright (c) 1997 Microsoft Co...	Copyright (c) 1997 Microsoft Corp.	1999/12/31	タイムスタンプ	Microsoft Timestam	
Device Management Root CA	Device Management Root CA	2052/03/14	<すべて>	<なし>	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	2031/11/10	クライアント認証, コ...	DigiCert	
DigiCert Global Root CA	DigiCert Global Root CA	2031/11/10	クライアント認証, コ...	DigiCert	
DigiCert Global Root G2	DigiCert Global Root G2	2038/01/15	クライアント認証, コ...	DigiCert Global Ro...	
DigiCert Global Root G3	DigiCert Global Root G3	2038/01/15	クライアント認証, コ...	DigiCert Global Ro...	
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	2031/11/10	クライアント認証, コ...	DigiCert	
DigiCert Trusted Root G4	DigiCert Trusted Root G4	2038/01/15	クライアント認証, コ...	DigiCert Trusted Ro...	
DST Root CA X3	DST Root CA X3	2021/09/30	クライアント認証, ドキ...	DST Root CA X3	
Duo Endpoint Validation Root C...	Duo Endpoint Validation Root CA 1	2030/10/04	<すべて>	<なし>	
Entrust Root Certification Auth...	Entrust Root Certification Authority	2026/11/28	クライアント認証, コ...	Entrust	
Entrust Root Certification Auth...	Entrust Root Certification Authorit...	2030/12/08	クライアント認証, コ...	Entrust.net	
Entrust.net Certification Authori...	Entrust.net Certification Authority...	2029/07/24	クライアント認証, コ...	Entrust (2048)	
FMC	FMC	2032/05/15	<すべて>	<なし>	
GlobalSign	GlobalSign	2029/03/18	クライアント認証, コ...	GlobalSign Root CA	

はい をクリックすると Internal CA の証明書がインポートされる
Microsoft 管理コンソール (MMC) からインポートされた証明書が確認可能 (参考情報)

ステップ3-1: SSL policy の作成

①

②

New SSL Policy

Name:
SSL-Policy

Description:

Default Action:
 Do not decrypt
 Block
 Block with reset

Cancel Save

③

- ① FMC にて Policies > SSL を選択
- ② New Policy をクリック
- ③ 以下を入力し Save
 - ポリシー名
 - Default Action はそのまま (Do not decrypt) で

本シナリオでは、簡素化のため、すべての通信において TLS 復号を行うポリシーを適用する。実際には、FTD の負荷軽減のためにも、複合する通信としないののメリハリ分けを

ステップ3-2: SSL policy のルール作成

SSL-Policy

Enter Description

Rules Trusted CA Certificates Undecryptable Actions

+ Add Category + Add Rule QSearch Rules

1

Name DECRYPT-ALL Enabled Insert into Category Standard Rules

Action Decrypt - Resign with FMC-CA Replace Key Only

Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging

Available Zones

- dmz
- inside
- outside

Add to Source Add to Destination

Source Zones (0) any

Destination Zones (0) any

2

- ① Add Rule をクリック
- ② 以下の設定を行う
 - Rule 名を作成し Enabled をクリック
 - Action を Decrypt - Resign に
 - 使用する FMC 証明書を選択

ステップ3-2: SSL policy のルール作成 (続き)

Add Rule

Name: DECRYPT-ALL Enabled Insert: into Category Standard Rules

Action: Decrypt - Resign with FMC-CA Replace Key Only

Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version **Logging**

Log at End of Connection

Send Connection Events to:

Firepower Management Center

Syslog Server (Using default syslog configuration in Access Control Logging) [Show Overrides](#)

SNMP Trap Select an SNMP Alert Configurat +

Cancel Add

- ③ Logging タブをクリック
- ④ 「Log at End of Connection」と「Firepower Management Center」をチェック
- ⑤ Add ボタンをクリック

ステップ3-3: SSL policy のルール作成 (続き)

SSL-Policy

You have unsaved changes **Save** **Cancel**

Enter Description

Rules Trusted CA Certificates Undecryptable Actions

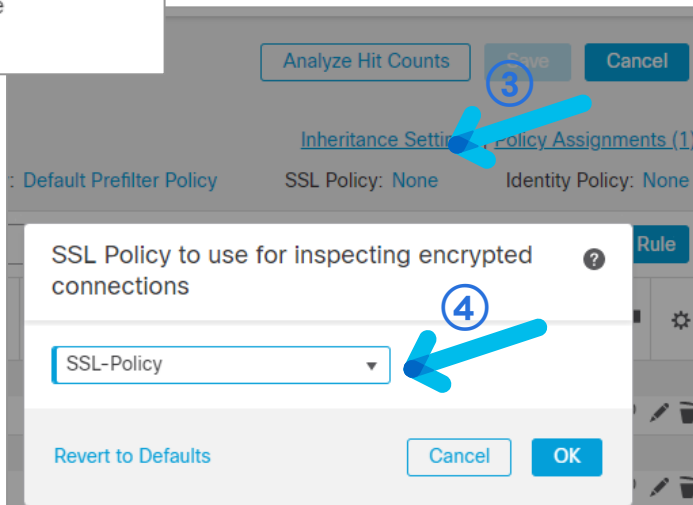
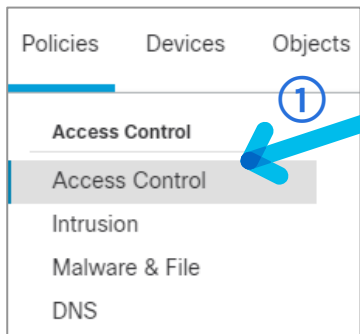
+ Add Category + Add Rule QSearch Rules X

#	Name	So... Zo...	D... Zo...	Sou... Net...	Dest Net...	V... T...	U...	Ap...	So... Pof...	Dest Por...	Cat...	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DECRYPT-ALL	any	any	any	any	any	any	any	any	any	any	any	→ Decrypt - Resign
Root Rules													
This category is empty													
Default Action												Do not decrypt	

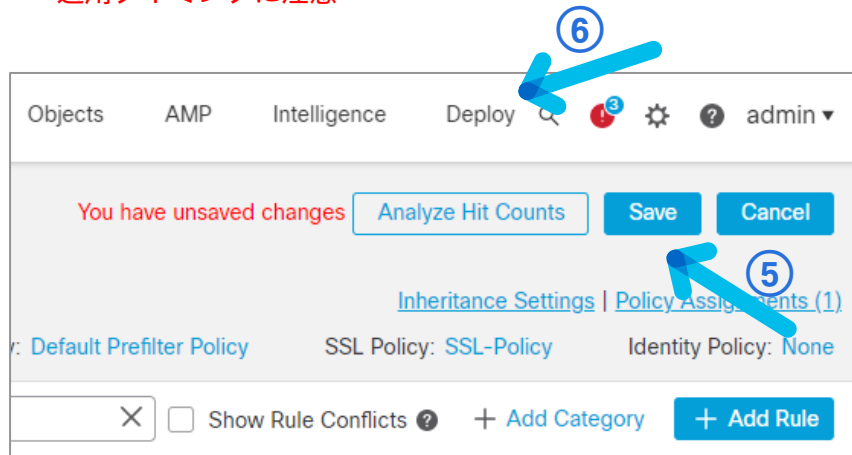
① 設定したルールに間違いがないことを確認した後、Save をクリック

ステップ4: Access Control Policy と SSL Policy の紐付けとデプロイ

- ① Policies > Access Control を選択
- ② FTD で利用している ACP の鉛筆アイコン (edit) をクリック
- ③ SSL Policy をクリック
- ④ 作成した復号ポリシーを選択し OKをクリック
- ⑤ ACP 画面に戻って Save をクリック
- ⑥ Deploy をクリックし 対象デバイスに設定適用 (※)

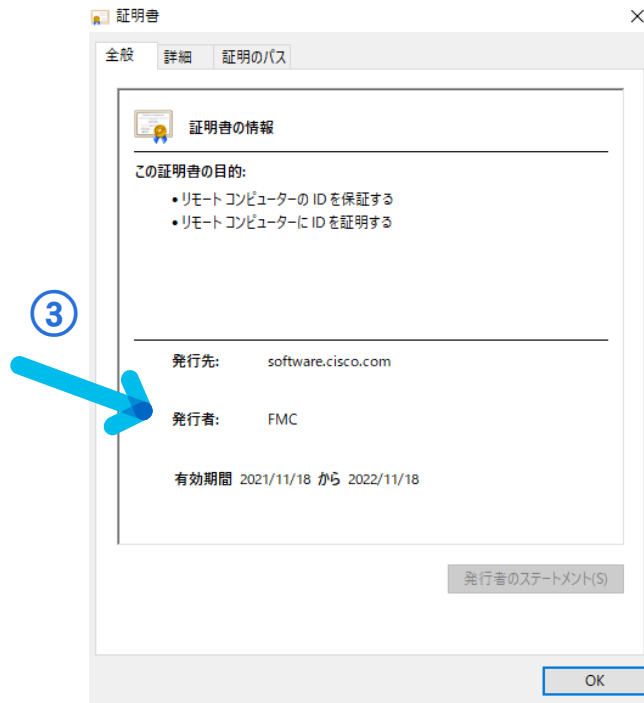


※SSLポリシーはデプロイ時 通信影響が発生するため
適用タイミングに注意

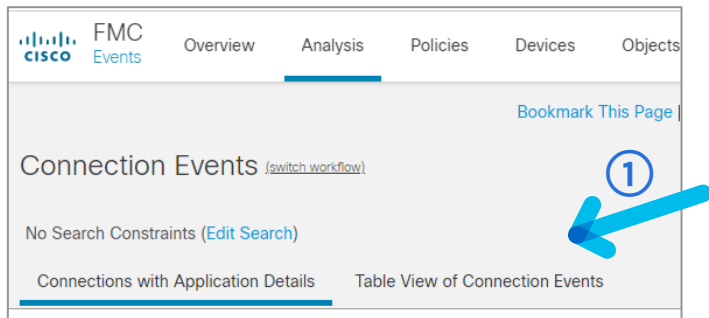


ステップ5-1: PC からの https サイトに疎通確認

Deploy 終了後、動作確認を行う。テスト PC の Web ブラウザ (今回は Chrome を使用) から任意の https サイトにアクセスし、アドレスバーの鍵マークをクリックすることで、どの証明書を使い暗号通信をしているか確認できる



ステップ5-2: FMCでイベント確認



FMC Events Overview Analysis Policies Devices Objects

Bookmark This Page

Connection Events [\(switch workflow\)](#)

No Search Constraints [\(Edit Search\)](#)

[Connections with Application Details](#) **Table View of Connection Events**

- ① FMC の Connection Events から、Table View を選択
- ② SSL Status という項目にて、その https の通信が復号 (outgoing の resign) されていることを確認できる



SSL Status ×	Application Protocol ×	Client ×	Client Version ×	Web Application ×	Application Risk ×	Business Relevance ×
🔒 Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Microsoft Windows Live Services Authentication	Medium	Low
🔒 Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Microsoft	Medium	Low
🔒 Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Microsoft Windows Live Services Authentication	Medium	Low
🔒 Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Microsoft Windows Live Services Authentication	Medium	Low
🔒 Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Microsoft Windows Live Services Authentication	Medium	Low
🔒 Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Microsoft Windows Live Services Authentication	Medium	Low
🔒 Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> Microsoft Windows Live Services Authentication	Medium	Low
🔒 Decrypt (Resign)	<input type="checkbox"/> HTTPS	<input type="checkbox"/> SSL client		<input type="checkbox"/> OneDrive	Medium	Medium

12. Identity(ID)FW の設定

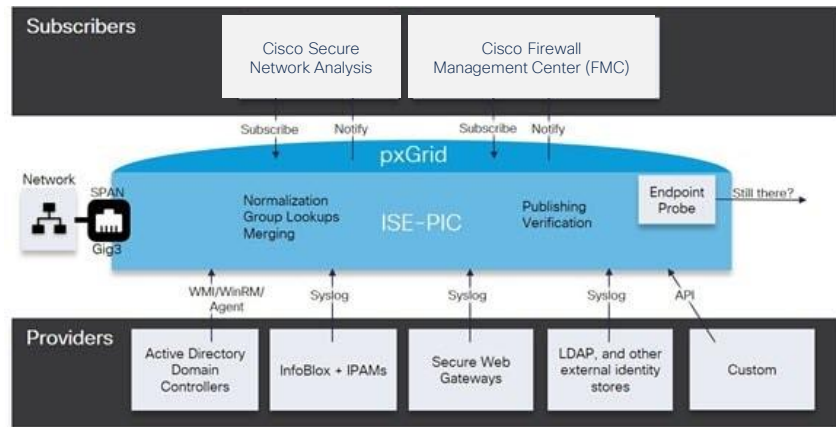
Identity Firewall 概要

- ユーザーアイデンティティ情報をトラフィックフローに関連付けることで可視性の強化、およびユーザ・グループベースでのトラフィック制御を実現
- 使用コンポーネント
 - Firepower Management Center (FMC)
 - Firepower Threat Defense (FTD)
 - Identity Source : ISE、または ISE Passive Identity Connector (ISE-PIC)
 - Identity Store : Active Directory、または LDAP
- FMC は Identity Source、および Identity Store からそれぞれ以下の情報を取得して、ユーザ情報の可視化およびポリシーに反映
 - Identity Source : ユーザと IP アドレスのマッピング情報を FMC に提供
 - Identity Store : FMC の Realm (レルム) で設定された AD または LDAP から取得されるユーザとグループ情報。ポリシー作成に利用。

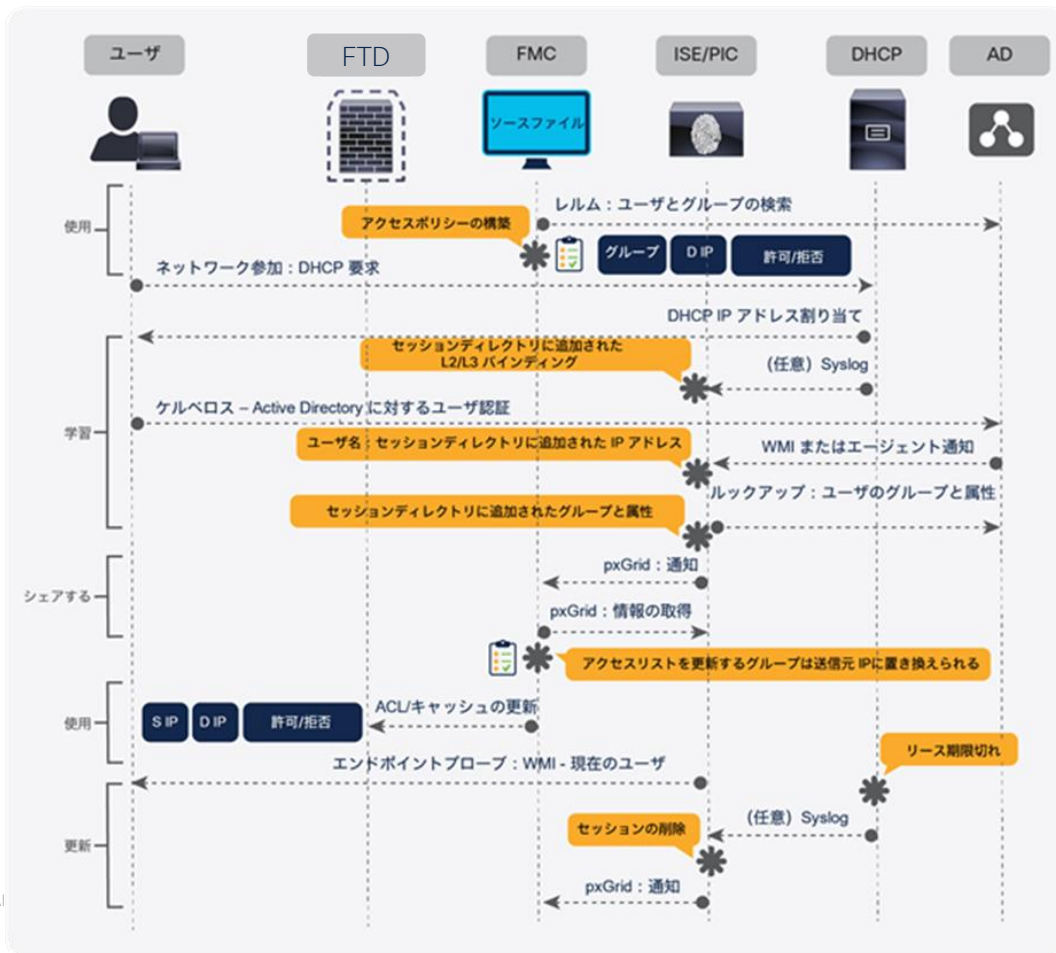
※注 : Firepower 7.0 Identity Source として User Agent は利用できない

ISE / ISE Passive Identity Connector (ISE-PIC)

- FMC の Identity Source として動作
- パッシブ認証によって AD より取得したユーザおよび IP のマッピング情報を pxGrid を介して FMC に送信
- ISE-PIC は ISE の簡易版 (安価版) であり、パッシブ認証に特化した製品
- パッシブ認証とは
 - 直接の認証行為を行わず、プロバイダと呼ばれる Microsoft Active Directory (AD) などの信頼されたサードパーティシステムからネットワーク上のユーザのユーザ ID や IP アドレスなどの属性情報をパッシブに学習する技術
 - ISE / ISE-PIC は WMI や DC 上にインストールされた ISE-PIC エージェントなどを使用して AD からドメインユーザのログインと更新の通知を受け取る
 - WMI の利用を推奨



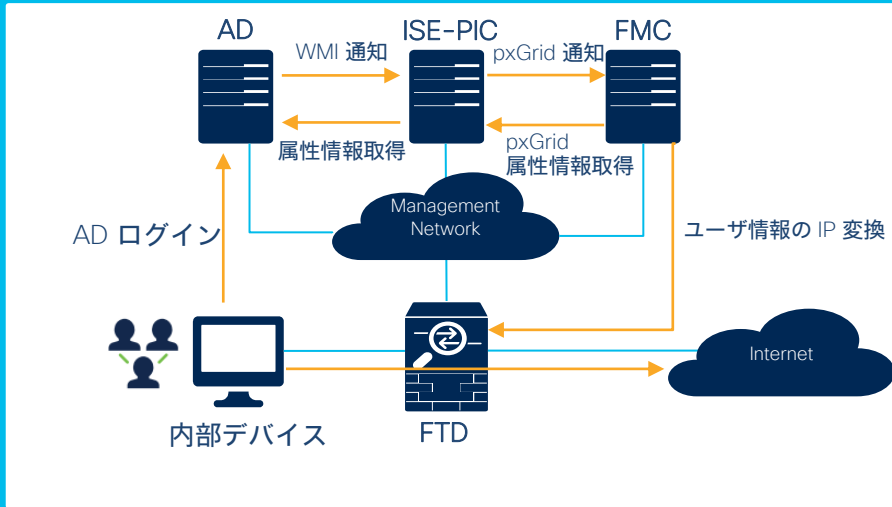
参考 : FMC - ISE / ISE-PIC ワークフロー



IDFW 設定ステップ

(FMC - ISE-PIC インテグレーション)

1. ISE-PIC のインストール、初期セットアップ
2. ISE-PIC での AD Join 設定
3. ISE-PIC での Root CA のダウンロードと FMC へのインポート
4. FMC での Internal CA の作成とダウンロード
5. OpenSSL による FMC Internal CA ファイルの形式変換 (PKCS#12 → PEM, Key)
6. FMC での Internal Cert のインポート
7. ISE-PIC での FMC Internal CA (PEM) のインポート
8. ISE-PIC での pxGrid の有効化
9. FMC での Identity Source の設定とテスト

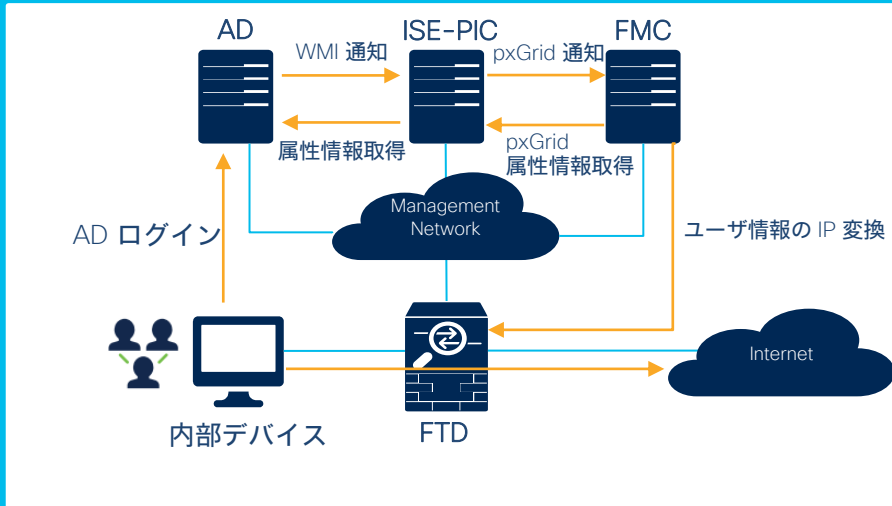


本ガイドでは Identity Source と
して ISE-PIC を使用

IDFW 設定ステップ

(FMC での Identity Policy 設定)

10. Realm の設定
11. Network Discovery での User の追加
12. Identity Policy の作成
13. ACP への Identity Policy の適用
14. 接続テスト



本ガイドでは Identity Source と
して ISE-PIC を使用

本セットアップガイドでの設定条件

- Identity Source として ISE-PIC v3.1 を利用
- Identity Store として AD (Windows Server 2016) を利用し (domain : secvt.jp)、Test PC1 をドメイン参加
- 必要コンポーネント (AD、ISE-PIC) はすでにインストール済みでありこのガイドでは解説しない
 - ISE-PIC Installation Guide
https://www.cisco.com/c/en/us/td/docs/security/ise/3-1/pic_install_upgrade/b_pic_install_upgrade_31.html
- FMC – ISE-PIC 間の pxGrid 連携で使用される証明書はそれぞれ自己証明書を使用
 - 証明書内に記載されている FQDN ホストの名前解決が行えるようADで設定済
- 本構成では管理ネットワークとユーザーネットワークのルーティングが行えないため、ユーザーネットワーク (192.168.1.0/24) と AD の通信経路を別途確保 (次頁構成図参照)
 - IDFW を利用しない環境においては、管理ネットワークとユーザーネットワークが分離されている方が望ましいデザインであり、本環境は本来は IDFW を利用するようなデザインにはなっていないため、一時的な対応として AD をマルチホームで運用

ネットワーク環境図 (再掲)

Internet

■ 設定済みの機器

MGMT NW

.135.254

DNS: 64.104.14.184

ntp.esl.cisco.com

proxy-wsa.esl.cisco.com

10.71.128.0/21

VM Network

.132.194

G0/0 outside .1

FTDv01

test PC2

Management

G0/1 inside .1

.101

.132.204

FMCv

.132.130

ISE-PIC01

.132.220

ESXi

.132.131

内部LAN
192.168.1.0/24

.11

.101

AD01.secvt.jp

test PC1

管理NW (実態はシスコ検証NW)

顧客NW

g0/0 グローバルアドレス

ASA

g0/3 .254

外部LAN

192.168.240.0/24

PAT

PAT

ISE-PIC での AD Join 設定

- ISE-PIC にてパッシブ ID サービスのプロバイダとなる AD を登録

Providers > Active Directory

- ① ISE-PIC にログイン後、左上のメニューアイコンをクリック
- ② Providers > Active Directory を選択
- ③ Add をクリック

The image shows a sequence of three screenshots from the ISE-PIC web interface, illustrating the steps to add an Active Directory provider. The first screenshot shows the main menu icon (hamburger menu) in the top left corner, highlighted with a red box and a blue arrow labeled '1'. The second screenshot shows the 'Providers' tab selected in the top navigation bar, with a red box and a blue arrow labeled '2'. The third screenshot shows the 'Active Directory' page, where the '+ Add' button is highlighted with a red box and a blue arrow labeled '3'. The page title is 'Providers · Active Directory' and the main heading is 'Active Directory'. Below the heading, there are buttons for 'Edit', '+ Add', and 'Delete', along with search and tool options. A table with one row is visible, containing a checkbox, the text 'Join Point', and 'Active Directory Domain'. The bottom of the page displays 'No data available'.

ISE-PIC での AD Join 設定

- ① 任意の名前を入力
- ② AD のドメインを入力
- ③ 右下の Submit をクリック
- ④ 登録したドメインにすべての ISE ノードを参加させるかのメッセージが表示されるため Yes をクリック
- ⑤ Domain Admin のユーザ ID / パスワードを入力
- ⑥ OK をクリック
- ⑦ ISE の Node Status が Completed になることを確認

ISE Passive Identity Connector Providers · Active Directory

Connection

* Join Point Name ⓘ

* Active Directory Domain ⓘ

i

Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No

Join Domain

Please specify the credentials required to Join node(s) to the Active Directory Domain.

* Domain Administrator ⓘ

* Password ⓘ

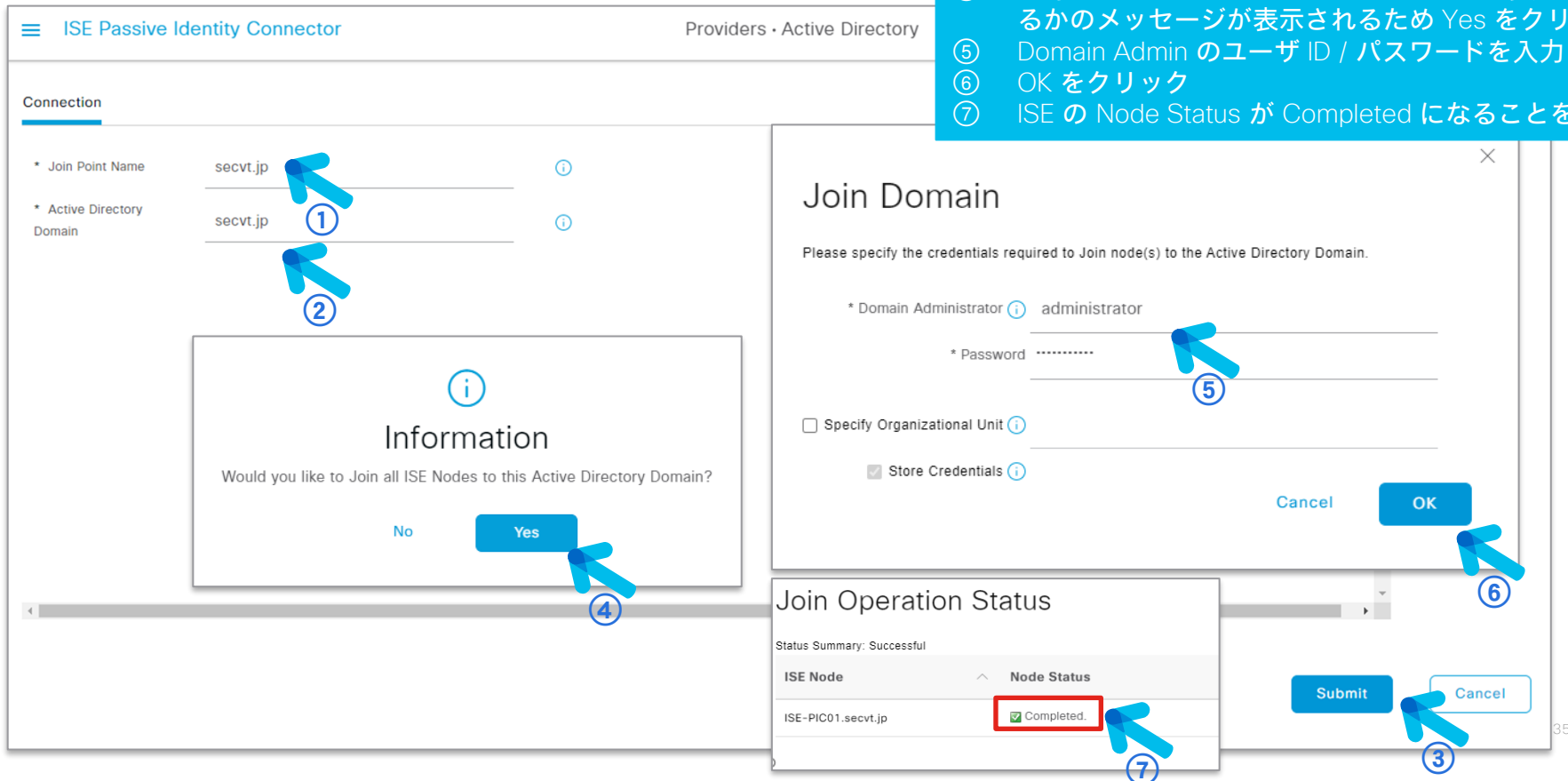
Specify Organizational Unit ⓘ

Store Credentials ⓘ

Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ISE-PIC01.secvt.jp	<input checked="" type="checkbox"/> Completed.



ISE-PIC での AD Join 設定

- 追加でパッシブ ID サービス設定を実施

- ① PassiveID を選択
- ② Add DCs を選択
- ③ 先ほど登録した secvt.jp ドメインが表示されるのでチェックを入れる
- ④ OK をクリック

ISE Passive Identity Connector Providers · Active Directory

Connection Allowed Domains **PassiveID** Groups Advanced Settings

PassiveID Domain Controler

Refresh Edit Trash **Add DCs** Use Existing Agent Config WMI Add Agent

Domain	DC Host	Site
<input checked="" type="checkbox"/>	secvt.jp	AD01.secvt.jp

No data found.

Add Domain Controllers

Domain	DC Host	Site	IP Address
<input checked="" type="checkbox"/>	secvt.jp	AD01.secvt.jp	Default-First-Site-Name 10.71.132.131

Cancel OK

ISE-PIC での AD Join 設定

・追加でパッシブ ID サービス設定を実施

- ① PassiveID DC に登録された secvt.jp を選択
- ② Edit を選択
- ③ AD admin の Password を入力
- ④ Protocol で WMI を選択して Configure をクリック
- ⑤ Information Successfully の Pop-up が出れば OK
- ⑥ Test をクリック
- ⑦ Information で Successfully の Pop-up が出れば OK
- ⑧ Save をクリック

ISE Passive Identity Connector Providers · Active Directory

Connection Allowed Domains **PassiveID** Groups Advanced Settings

PassiveID Domain Controllers

Rows/Page 1

Refresh Edit Trash Add DCs Use Existing Agent Config WMI Add Agent

Domain	DC Host	Site	IP Address
<input checked="" type="checkbox"/> secvt.jp	AD01.secvt.jp	Default-First-Site-Name	10.71.132.131

Edit Item
Edit Domain Controller

Host FQDN
AD01.secvt.jp

Description

User Name*
administrator

Password
.....

Protocol
WMI

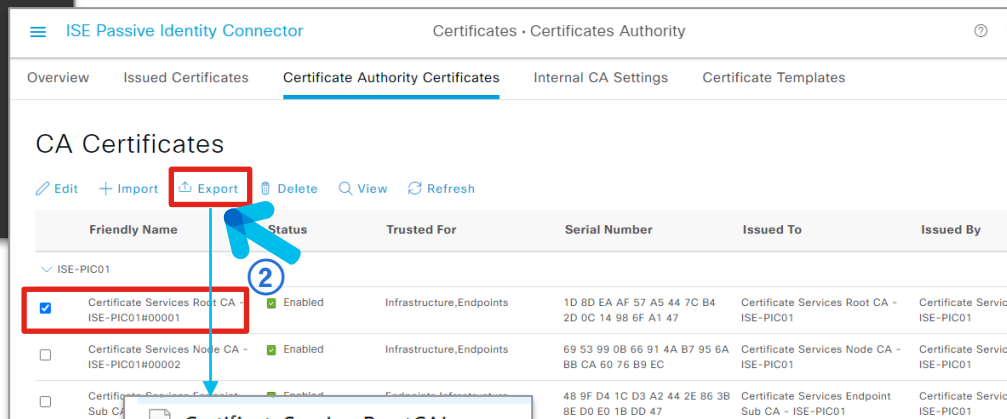
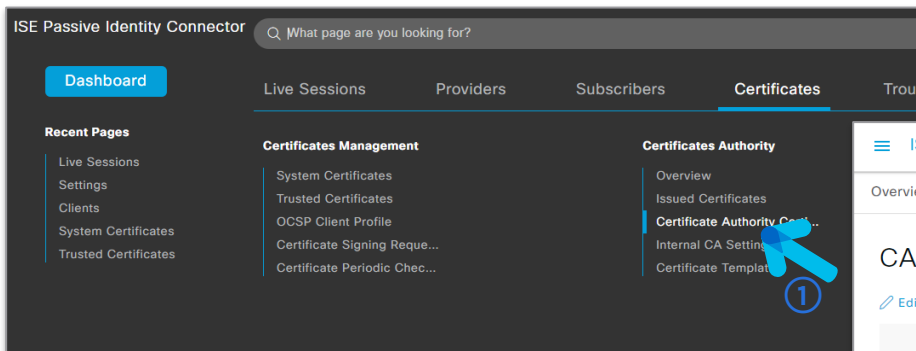
Configure Test Cancel Save

Information
Successfully configured Domain Controller
OK

Information
The connection was tested on 'ISE-PIC01.secvt.jp' PassiveID active node.
Connection to 'AD01.secvt.jp' established successfully.
Windows version is 'Win2016'; NetBIOS domain is 'SECVT'. Query for history events succeeded.
OK

ISE-PIC での Root CA のダウンロードと FMC へのインポート

- ISE-PIC – FMC 間は証明書を用いてセキュアな接続を行う。今回自己証明書を使用するため、はじめに ISE-PIC の Root CA (自己証明書) をダウンロードして FMC にインポートする
Certificates > Certificates Authority > Certificates Authority Certificates



- ISE-PIC メニューより Certificate Authority Certificates をクリック
- Root CA を選択し、Export をクリック

FMC での Internal CA の作成およびダウンロード

- FMC Internal CA は 11章 “TLS Decryption の設定” で作成済のためそれを活用する

Objects > Object Management > PKI > Internal CAs

Firepower Management Center
Objects / Object Management

Internal CAs

Name	Value
FMC-CA	CN=FMC, ORG=CiscoSystemsGK, OU=GSSO-...

- ① 作成済の FMC-CA の編集ボタンをクリック
- ② Download をクリック
- ③ Encrypt Download File でパスワードをセット
- ④ OK をクリック
- ⑤ Cancel をクリック
- ⑥ Download したファイル名をわかりやすい名前に変更しておく

e5f35e4a-ba43-11ec-bafe-82fc29d353f1.p12

FMCv01.p12

OpenSSL による FMC Internal CA ファイルの形式変換 (PKCS#12 → PEM, Key)

- FMC Internal CA の ISE-PIC へのインストールのためにファイル形式の変換 (PKCS#12 → PEM) が必要。また、ISE-PIC との接続に FMC は Internal Cert の証明書を使用し、作成済 Internal CA 証明書を Internal Cert にもインポートする必要があるが、こちらもインポートに PEM ファイルと秘密鍵がそれぞれ必要になるため、OpenSSL ソフトを利用して PKCS#12 ファイルからファイル形式を変換する
- 以下のサイトより Windows 10 版の OpenSSL をダウンロードし、端末にインストール

- <https://slproweb.com/products/Win32OpenSSL.html>

- 本ガイドでは Win64 OpenSSL v1.1.1o Light を利用

- FMCv01.p12 が存在するディレクトリ上で以下のコマンドを実行

Win64 OpenSSL v1.1.1o Light EXE MSI	3MBインストーラー	Win64 Op れはOpen
Win64 OpenSSL v1.1.1o	43MBインストーラー	Win64 Op

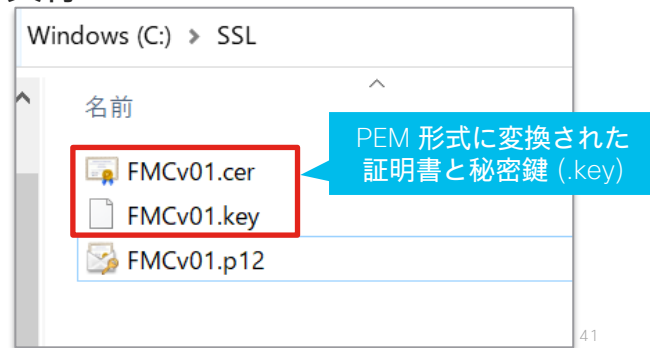
```
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sinazawa>cd C:\ssl

C:\SSL>openssl pkcs12 -nokeys -clcerts -in FMCv01.p12 -out FMCv01.cer
Enter Import Password:

C:\SSL>openssl pkcs12 -nocerts -in FMCv01.p12 -out FMCv01.key
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

C:\SSL>
```



FMC での Internal Cert のインポート

Add Known Internal Certificate

Name:

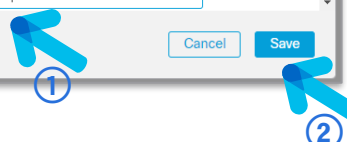
Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDIDCCAnygAwIBAgIUOELFNnOrxXizxPUCgZW22VNxY6EwDQYJKoZIhvcNAQEL
BQAwajELMAkGA1UEBhMCStAxJjAMBgNVBAgMBVRva3lvMRIwEAYDVQQHDAlNa
W5h
dG8ta3UxZmFzAVBgNVBAoMDkNpc2NvU3lzdGVtc0dLMRAwDgYDVQQLDAdHU1NPL
UpQ
-----END CERTIFICATE-----
```

Key or, choose a file:

```
IwnoVxx4JuPSdCz9PyAvq4rdh4ExDZVu6MCw3dZLfgTlYjPvTeEYCZK1TCgIWF
s1u62oIIATnN/4f9IEPIsVZBYmZMniw6feTAvhbVoGwEbaagK/btyzT7GixuDSM
sf7i2UISf9zkSLNH/9uwZjcDQZz2klPsrFCYYZHVozALV6b95eedHKDaUv8Qla1S
TKTjypga+qGOPjDExcVwfm890XCsgoIVkK:5axxF9mi8WAh831Ryh1Lvmn6020Ti
jU8tPBikD22WFGyVrP2ypQ==
-----END ENCRYPTED PRIVATE KEY-----
```

Encrypted, and the password is:



Internal Certs

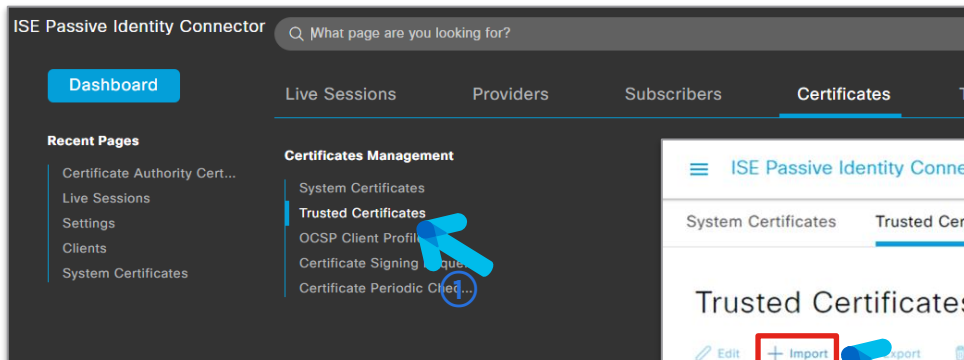
Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Name	Value	
FMCv01	CN=FMC, ORG=CiscoSystemsGK, OU=GSSO-...	

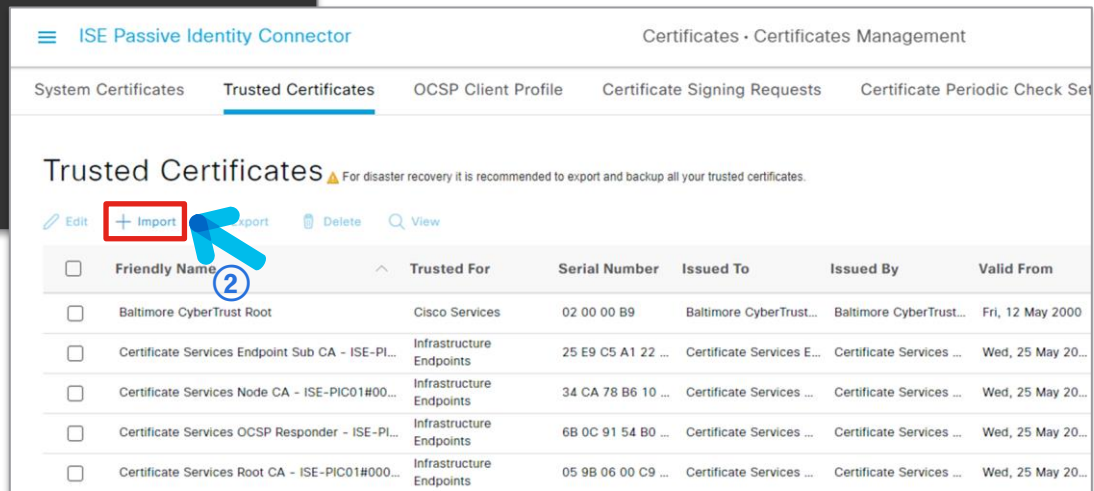
- ① Encrypted にチェックを入れてパスワードをセット
- ② Save をクリック

ISE-PIC での FMC Internal CA のインポート

- ISE-PIC にて FMC の Internal CA (変換した PEM ファイル) をインポート
Certificates > Certificates Management > Trusted Certificates



- ① ISE-PIC のメニューより Certificates > Certificates Management > Trusted Certificates を選択
- ② Import をクリック



ISE-PIC での FMC Internal CA のインポート

ISE Passive Identity Connector Certificates - Certificates Management

System Certificates **Trusted Certificates** OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Settings

Import a new Certificate into the Certificate Store

* Certificate File FMCv01.cer

Friendly Name FMCv01-Cert

Trusted For:

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for certificate based admin authentication
- Trust for authentication of Cisco Services
- Validate Certificate Extensions

Description

① Certificate File でファイルを選択をクリックして FMCv01.cer を選択
② 任意の名前を入力
③ Trust for authentication within ISE にチェックが入っていることを確認
④ Submit をクリック

ISE-PIC での pxGrid の有効化

- ISE-PIC にて pxGrid 連携でサブスクリバとなる FMC からの接続を許可するための設定を行う

Subscribers > Settings

- ① ISE-PIC のメニューより Subscribers > Settings を選択
- ② Automatically approve new certificate-based accounts にチェック
- ③ Save をクリック

The screenshot displays the ISE Passive Identity Connector web interface. The top navigation bar includes 'Dashboard', 'Live Sessions', 'Providers', 'Subscribers', 'Certificates', 'Troubleshoot', 'Reports', and 'Administration'. The 'Subscribers' menu item is selected, and the 'Settings' option is highlighted with a red box and a blue arrow labeled '①'. Below this, the 'Settings' page is shown with the following configuration options:

- Automatically approve new certificate-based accounts ①
- Allow password based account creation ①

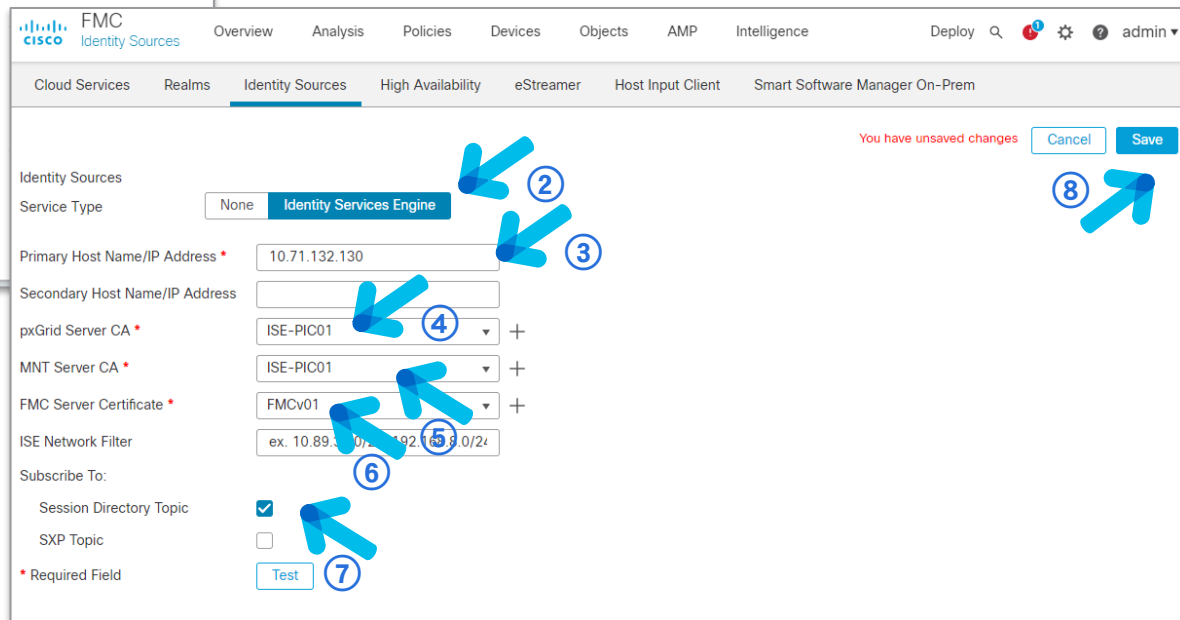
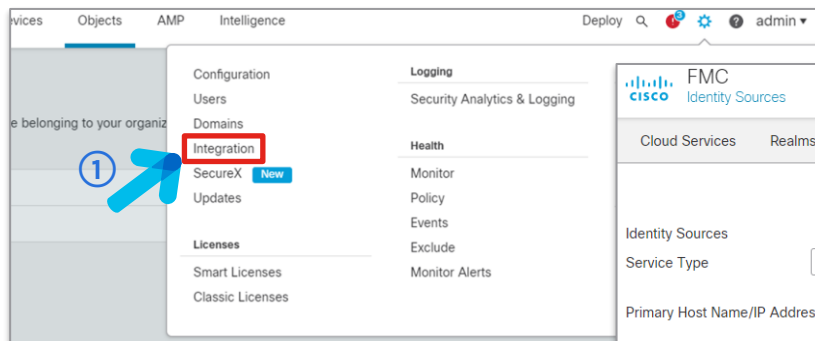
At the bottom of the settings page, there are 'Use Default' and 'Save' buttons. A blue arrow labeled '②' points to the 'Automatically approve new certificate-based accounts' checkbox, and another blue arrow labeled '③' points to the 'Save' button.

FMC での Identity Source の設定

- 最後に FMC の Identity Source の設定を実施

System > Integration > Identity Source

- ① Integration を選択
- ② Service Type で Identity Services Engine を選択
- ③ ISE-PIC の IP アドレスを入力
- ④ pxGrid Server CA で ISE-PIC01 を選択
- ⑤ MNT Server CA で ISE-PIC01 を選択
- ⑥ FMC Server Certificate で FMCv01 を選択
- ⑦ Subscribe To で Session Directory Topic にチェックが入っていることを確認
- ⑧ Save をクリック



FMC – ISE-PIC 連携テスト

FMC Identity Sources

Overview Analysis Policies Devices Objects

Cloud Services Realms Identity Sources High Availability eStreamer

Identity Sources

Service Type: None Identity Services Engine

Primary Host Name/IP Address * 10.71.132.130

Secondary Host Name/IP Address

pxGrid Server CA * ISE-PIC01 +

MNT Server CA * ISE-PIC01 +

FMC Server Certificate * FMCv01 +

ISE Network Filter ex. 10.89.31.0/24, 192.168.8.0/24

Subscribe To:

Session Directory Topic

SXP Topic

* Required Field Test

Status

ISE connection status:
Primary host: Success

Additional Logs

Primary host:
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ISE-PIC01.secv1.jp:8910
[INFO]: pxgrid 2.0: ISE server reports com.cisco.ise.config.profiler is unsupported or disabled

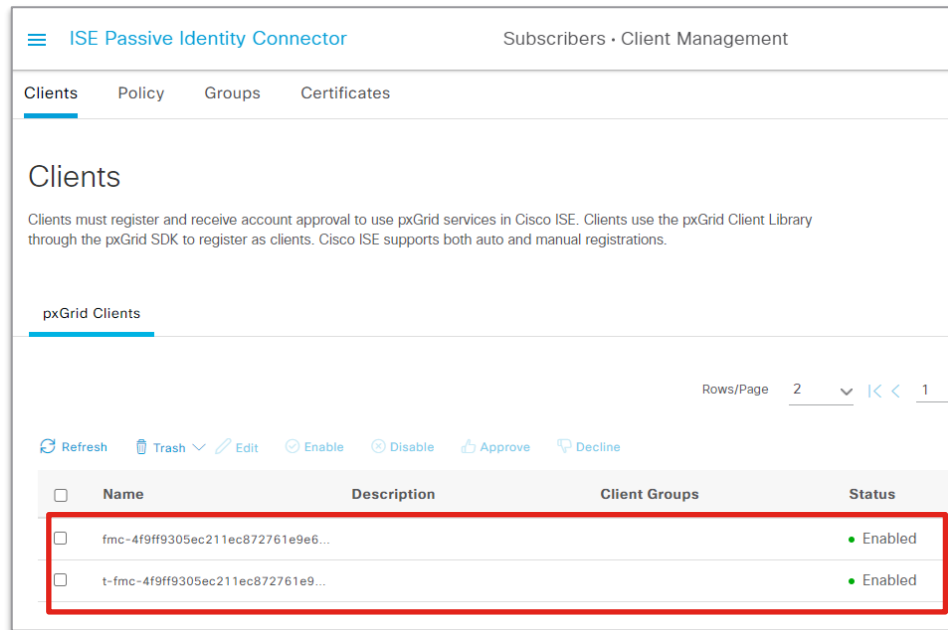
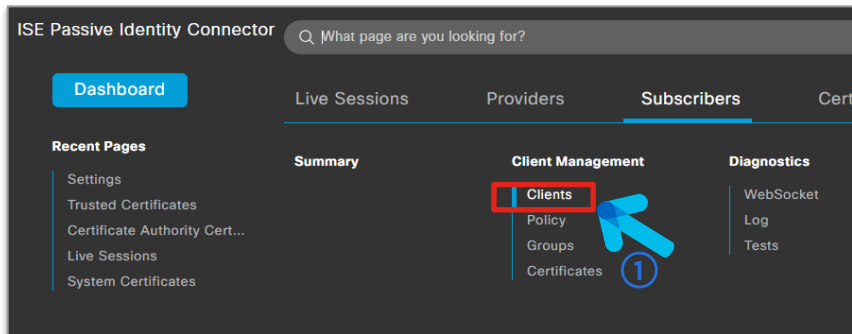
OK

- ① Test をクリック
- ② Primary host: Success と表示されればテスト成功

FMC - ISE-PIC 連携テスト

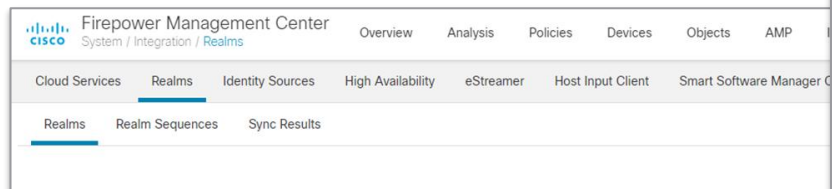
- ISE-PIC での接続確認

Subscribers > Clients



FMC での Realm (レルム) 設定

- ・ 選択したユーザーとグループを使ってポリシー設定を行うために FMC で AD Realm の作成を実施
System > Integration > Realms



Add New Realm

Name* AD01 Description

Type AD AD Primary Domain secvt.jp
E.g. domain.com

Directory Username* administrator@secvt.jp Directory Password*
E.g. user@domain.com

Base DN dc=secvt,dc=jp Group DN
E.g. ou=group,dc=cisco,dc=com E.g. ou=group,dc=cisco,dc=com

Directory Server Configuration

10.71.132.131:389

Hostname/IP Address* 10.71.132.131 Port* 389

Encryption None CA Certificate Select certificate

Interface used to connect to Directory server

Resolve via route lookup
 Choose an interface
Default: Management/Default interface

Test Test connection succeeded

Add another domain

Cancel Configure Groups and Users

- ① Add Realm をクリック
- ② 任意の名前を入力
- ③ Type で AD を選択
- ④ AD Primary Domain で secvt.jp を入力
- ⑤ ディレクトリ参照用のユーザ名/パスワードを入力。ユーザ名は @ domain の形式
- ⑥ Base DN を入力
- ⑦ Directory Server Configuration に移動し、AD01 の IP アドレスを入力
- ⑧ Encryption を今回は None で設定
- ⑨ Resolve via route lookup を選択
- ⑩ Test をクリックし接続が成功することを確認
- ⑪ Configure Groups and Users をクリック

FMC での Realm (レルム) 設定

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy

AD01

You have unsaved changes Save

Enter description

Group and User Sync Directory **Realm Configuration**

AD Primary Domain

secvt.jp
E.g. domain.com

Enter query to look for users and groups

Enter the directory tree on the server where the Firepower Management Center should begin searching for user and group data.

Base DN Group DN

dc=secvt,dc=jp dc=secvt,dc=jp
E.g. ou=group,dc=cisco,dc=com E.g. ou=group,dc=cisco,dc=com

Load Groups

Available Groups

Limit the groups to use in policy by moving them to either the Included Groups or Excluded Groups list. Moving one group to the Included Groups list, for example, allows that group only to be used in policy. [Learn more](#)

Available Groups (All groups are included by default)

Search

Sales
DnsUpdateProxy
DnsAdmins
Enterprise Key Admins

Included Groups and Users

Sales

Excluded Groups and Users

None

Include Exclude

- ① Available Groups に AD01 で定義されているグループが表示されていることを確認 ※表示されていない場合には Load Groups をクリックし改めて情報を取得
- ② Available Groups から Sales を選択して Include をクリック ※Available Groups で Included に選択されたグループ情報およびそのグループに所属する情報のみを AD から取得するようフィルタすることが可能。逆に Excluded を選択するとそのグループを除外することが可能
- ③ Save をクリック

Network Discovery での User の追加

- Identity Source の連携に伴い、作成済の Network Discovery Policy ルールにて Users を追加していなければこれを追加する

Policies > Network Discovery > Networks

The screenshot displays the Cisco Firepower Management Center interface. The main navigation bar includes 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is active, and the 'Networks' sub-tab is selected. A modal dialog titled 'Edit Rule' is open, showing a 'Discover' rule configuration. The 'Discover' dropdown is set to 'Discover', and the 'Hosts', 'Users', and 'Applications' checkboxes are all checked. A blue callout box with three numbered steps (1, 2, 3) provides instructions: 1. Click the edit button for the 'Discover: Hosts, Applications' rule. 2. Check the 'Users' checkbox. 3. Click the 'Save' button. The background shows the 'Policies' tab with 'Networks' selected, and a list of networks including '192.168.1.0_inside_hosts'.

Identity Policy の設定

- 新規に Identity Policy を作成する

Policies > Access Control > Identity

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is selected. The main content area shows a table with columns for 'Identity Policy', 'Domain', 'Status', and 'Last Modified'. A 'New Policy' button is visible in the top right corner. A dialog box titled 'New Identity policy' is open, showing a 'Name' field with 'ID-Policy' entered and a 'Description' field. The 'Save' button is highlighted with a blue arrow and a circled '3'. The 'New Policy' button in the background is also highlighted with a blue arrow and a circled '1'. The 'Name' field is highlighted with a blue arrow and a circled '2'.

- ① New Policy をクリック
- ② 任意のポリシー名を入力
- ③ Save をクリック

Identity Policy の設定

- 作成した Identity Policy にルールを追加する

Firepower Management Center
Policies / Access Control / Identity Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy Search Settings Help admin

ID-Policy

Enter Description

Save Cancel

Rules Active Authentication Identity Source

+ Add Category + Add Rule Search Rules X

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules										
This category is empty										
Standard Rules										
This category is empty										
Root Rules										
This category is empty										

Add Rule

Name: ISE-Authentication Enabled

Insert: into Category Standard Rules

Realm: No realm Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Remote access VPN sessions are authenticated by VPN. Other sessions use the rule Action.

Zones Networks VLAN Tags

Available Zones: Inside_Zone, Outside_Zone

Source Zones (1): Inside_Zone

Destination Zones (1): Outside_Zone

Buttons: Add to Source, Add to Destination, Cancel, Add

- 1 Add Rule をクリック
- 2 任意のルール名を入力
- 3 Passive Authentication を選択
- 4 Zones タブの Available Zones から Inside_Zone を選択して Add to Source をクリック
- 5 同様に Outside_Zone を選択して Add to Destination を選択

Identity Policy の設定

- 作成した Identity Policy にルールを追加する

Add Rule

Name: ISE-Authentication Enabled Insert: into Category Standard Rules

Passive Authentication Realm: AD01 (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Remote access VPN sessions are actively authenticated by VPN. Other sessions use the rule Action.

Zones Networks VLAN Tags Ports **Realm & Settings**

Realm * AD01 (AD) ①

Use active authentication if passive or VPN identity cannot be established

* Required Field

Cancel Add ②

- ① Realm & Settings タブに移動し Realm で AD01 を選択
- ② Add をクリック
- ③ Save をクリック

admin

You have unsaved changes Save Cancel ③

Rules Active Authentication Identity Source

+ Add Category + Add Rule Search Rules

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules										
This category is empty										
Standard Rules										
1 ISE-Authentication	Inside_Zone (Routed)	Outside_Zone (Routed)	any	any	any	any	any	AD01 (AD)	Passive Authentication	none
Root Rules										
This category is empty										

ACP への Identity Policy の適用

- 作成した Identity Policy を既存 ACP に適用する

Policies > Access Control > Access Control

The screenshot shows the Firepower Management Center interface. The main table lists Access Control Policies (ACP-1) with columns for Name, Domain, Status, and Last Modified. A red box highlights the edit icon (pencil) for ACP-1, labeled with a circled 1. A blue arrow points to this icon.

Below the table, a modal window titled "Identity Policy" is open. It shows a dropdown menu with "ID-Policy" selected, labeled with a circled 3. A blue arrow points to this dropdown. The "OK" button is highlighted with a blue arrow and labeled with a circled 4. A blue arrow labeled with a circled 2 points to the "Identity Policy: None" text in the "Policy Assignments" section of the modal.

At the bottom, a confirmation dialog is shown with the "Save" button highlighted by a blue arrow and labeled with a circled 5. The "Identity Policy: ID-Policy" is highlighted with a red box in the "Policy Assignments" section of this dialog.

On the right side, a blue box contains the following instructions:

- 1 ACP-1 の編集ボタンをクリック
- 2 右上の Identity Policy の None をクリック
- 3 作成したポリシー、ID-Policy を選択
- 4 OK をクリック
- 5 Save をクリック

設定の FTD への展開

Firepower Management Center
Deploy / Deployment

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 1 admin

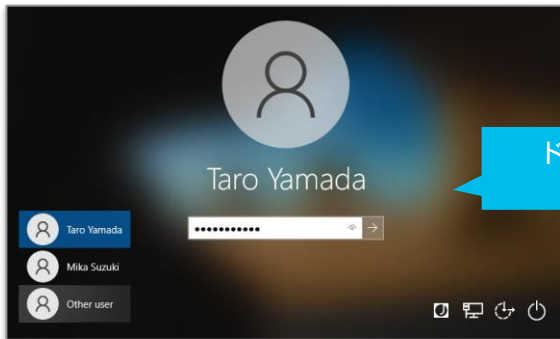
1 device selected
Deploy time: Estimate Deploy

Search using device name, user name, type, group or status

<input checked="" type="checkbox"/>	Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
> <input checked="" type="checkbox"/>	FTDv01	admin		FTD		May 27, 2022 11:51 AM		Pending

① Deploy をクリックして設定内容を FTDv01 に適用

接続テスト & Monitoring Events



ドメインユーザで
ログイン

• Analysis > Users > Active Sessions

• Analysis > Users > User Activities

Firepower Management Center
Analysis / Users / User Activity

Overview Analysis Policies Devices Objects AMP Intelligence

No Search Constraints ([Edit Search](#))

Table View of Events Users

	Time x	Event x	Username x	Realm x	Discovery Application x	Authentication Type x	IP Address x	Start Port x	End Port x	Description x	VP Se Ty
<input type="checkbox"/>	2022-06-01 10:20:49	User Login	tyamada	AD01	LDAP	Passive Authentication	192.168.1.101				

<< Page 1 of 1 >> Displaying row 1 of 1 rows

[View](#) [Delete](#)
[View All](#) [Delete All](#)

Firepower Management Center
Analysis / Users / Active Sessions

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy [Search](#) [Settings](#) [Help](#) admin

[Bookmark This Page](#) | [Reporting](#) | [Dashboard](#) | [View Bookmarks](#) | [Search](#) [Predefined Searches](#)

No Search Constraints ([Edit Search](#))

Table View of Active Sessions Active Sessions

Jump to...

	Login Time x	Last Seen x	User x	Authentication Type x	Current IP x	Realm x	Username x	First Name x	Last Name x	E-Mail x	Department x	Phone x	Discovery Application x	Device x
<input type="checkbox"/>	2022-06-01 10:20:49	2022-06-01 10:25:15	taro yamada (AD01\tyamada, LDAP)	Passive Authentication	192.168.1.101	AD01	tyamada	taro	yamada	tyamada@secvt.jp	users (secvt)		LDAP	FMCv01
<input type="checkbox"/>	2022-05-31 08:33:46	2022-06-01 04:03:47	AD01\administrator (LDAP)	Passive Authentication	10.71.132.131	AD01	administrator				users (secvt)		LDAP	FMCv01
<input type="checkbox"/>	2022-05-31 00:01:17	2022-06-01 07:55:21	AD01\administrator (LDAP)	Passive Authentication	10.71.132.130	AD01	administrator				users (secvt)		LDAP	FMCv01

[View](#) [Delete](#)
[View All](#) [Delete All](#)

接続テスト & Monitoring Events

- Analysis > Users > Active Sessions

ブラウザから Web アクセス

注: ドメインユーザへの TLS 復号許可のため別途 FMC CA を PC にインポート済

Firepower Management Center Analysis / Users / Active Sessions

Jump to...
Connection Events
Security Intelligence Events
Intrusion Events
Malware Events

Firepower Management Center Analysis / Connections / Events

Connection Events
Table View of Connection Events

Firepower Management Center Analysis / Connections / Events

Connection Events

Table View of Connection Events

Connection Events でユーザ情報がマッピングされていることを確認

	First Packet	Action	Initiator IP	Initiator User	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Destination Port / ICMP Code	SSL Status	Application Protocol	Client	Client Version	Web Application	Application Risk
▼	2022-06-01 10:52:26	Allow	192.168.1.101	taro yamada (AD01\tyamada, LDAP)	104.18.103.56	USA	Inside_Zone	Outside_Zone	443 (https) / tcp	Decrypt (Resign)	HTTP/2	Chrome	101.0.4951.67	Box	Medium
▼	2022-06-01 10:52:25	Allow	192.168.1.101	taro yamada (AD01\tyamada, LDAP)	104.18.103.56	USA	Inside_Zone	Outside_Zone	443 (https) / tcp	Decrypt (Resign)	HTTP/2	Chrome	101.0.4951.67	Box	Medium

接続テスト & Monitoring Events

- Analysis > Users > Active Sessions

```
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\tyamada>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=4ms TTL=56
Reply from 1.1.1.1: bytes=32 time=4ms TTL=56
Reply from 1.1.1.1: bytes=32 time=4ms TTL=56
Reply from 1.1.1.1: bytes=32 time=12ms TTL=56

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 12ms, Average = 6ms

C:\Users\tyamada>
```

端末から 1.1.1.1 へのPing

Firepower Management Center Analysis / Users / Active Sessions

Jump to...
Connection Events
Security Intelligence Events
Intrusion Events
Malware Events

Table View of Active Sessions Active Sessions

<input type="checkbox"/>	↓ Login Time x	Last Seen x	User x	Auth
<input checked="" type="checkbox"/>	2022-06-01 10:20:49	2022-06-01 10:25:15	taro yamada (AD01\tyamada, LDAP)	Pass
<input type="checkbox"/>	2022-05-31 08:33:46	2022-06-01 04:03:47	AD01\administrator (LDAP)	Pass
<input type="checkbox"/>	2022-05-31 00:01:17	2022-06-01 07:55:21	AD01\administrator (LDAP)	Pass

Events By Priority and Classification

Search Constraints (Edit Search Save Search)

Drilldown of Event, Priority, and Classification Table View of Events Packets

Jump to...

- Message
- PROTOCOL-ICMP Unusual PING detected (1:29456:3)
- PROTOCOL-ICMP PING (1:384:8)

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence

Deploy Search admin

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search Predefined Searches

Events By Priority and Classification

Search Constraints (Edit Search Save Search)

Drilldown of Event, Priority, and Classification Table View of Events Packets

Jump to...

<input type="checkbox"/>	↓ Time x	Priority x	Impact x	Source IP x	Destination IP x	Destination Country x	Source Port / ICMP Type x	Destination Port / ICMP Code x	Message x	Classification x	Source User x	Application Protocol x	Client x
<input type="checkbox"/>	2022-06-01 10:59:32	medium	2	192.168.1.101	1.1.1.1	AUS	8 (Echo Request) / icmp	0 (No Code) / icmp	PROTOCOL-ICMP Unusual PING detected (1:29456:3)	Information Leak	taro yamada (AD01\tyamada, LDAP)	ICMP	ICMP client
<input type="checkbox"/>	2022-06-01 10:59:32	low	2	192.168.1.101	1.1.1.1	AUS	8 (Echo Request) / icmp	0 (No Code) / icmp	PROTOCOL-ICMP PING (1:384:8)	Misc Activity	taro yamada (AD01\tyamada, LDAP)	ICMP	ICMP client

Intrusion Events でユーザ情報がマッピングされていることを確認

Monitoring Events

- Unified Events

Filter columns

Select none | Select default

- Event Type
- Action
- Source User
- Source IP
- Destination IP

ユーザ名が画面に表示されていない場合には Filter columns をクリックして Source User をチェック

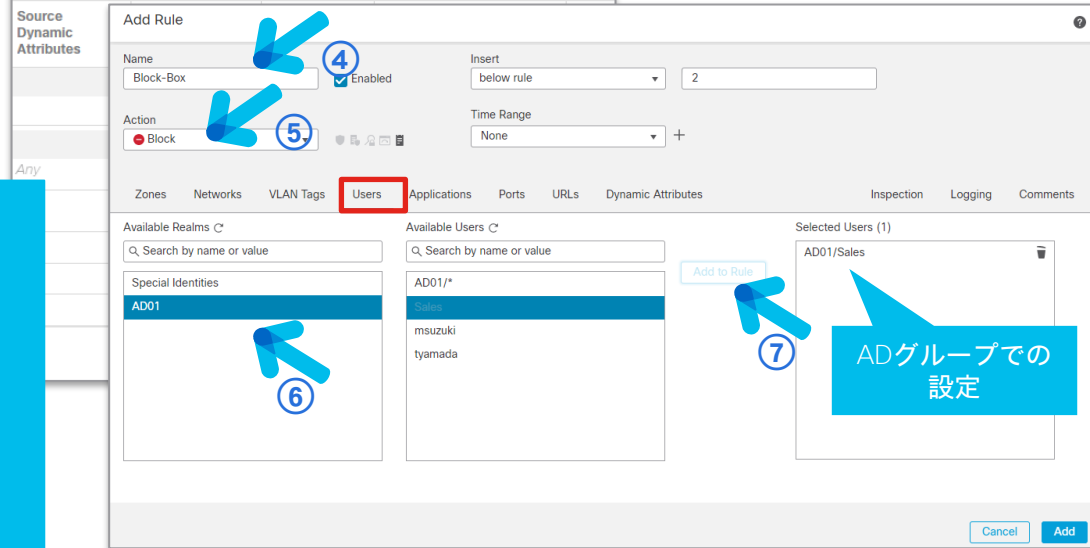
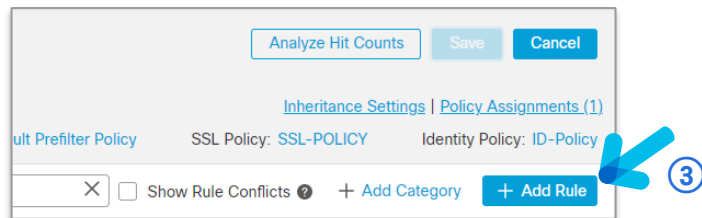
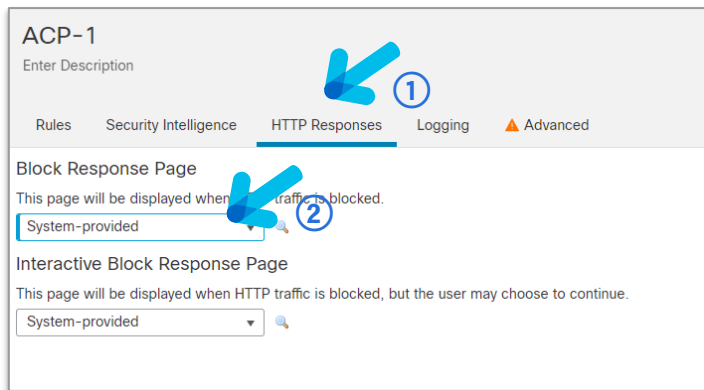
Showing all 1,510 events (🔍 1,464 📄 2 📄 44) ↓

📅 2022-06-01 10:07:28 JST → 2022-06-01 11:07:28 JST 1h 🔄 Go Live

Time	Event Type	Action	Source User	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Action
2022-06-01 11:04:01	Connection	Monitor	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.119.249.228	53439 / tcp	443 (https) / tcp	Microsoft	URL-MONITOR	AC
2022-06-01 11:04:01	Connection	Monitor	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.119.249.228	53438 / tcp	443 (https) / tcp	Microsoft	URL-MONITOR	AC
2022-06-01 11:04:01	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53437 / tcp	443 (https) / tcp	Microsoft Windows Live S	CATCH-ALL, URL-MONITOR	AC
2022-06-01 11:04:00	Connection	Monitor	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.119.249.228	53436 / tcp	443 (https) / tcp	Microsoft	URL-MONITOR	AC
2022-06-01 11:04:00	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53435 / tcp	443 (https) / tcp	Microsoft Windows Live S	URL-MONITOR, CATCH-ALL	AC
2022-06-01 11:03:43	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	104.46.162.226	53433 / tcp	443 (https) / tcp	Microsoft	CATCH-ALL	AC
2022-06-01 11:03:43	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53432 / tcp	443 (https) / tcp	Microsoft Windows Live S	CATCH-ALL, URL-MONITOR	AC
2022-06-01 11:03:43	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53431 / tcp	443 (https) / tcp	Microsoft Windows Live S	URL-MONITOR, CATCH-ALL	AC
2022-06-01 11:03:43	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	20.190.141.36	53430 / tcp	443 (https) / tcp	Microsoft Windows Live S	CATCH-ALL, URL-MONITOR	AC
2022-06-01 11:03:34	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	52.139.250.253	53429 / tcp	443 (https) / tcp	Microsoft	CATCH-ALL, URL-MONITOR	AC
2022-06-01 11:03:33	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.90.189.152	53428 / tcp	443 (https) / tcp	Microsoft	CATCH-ALL, URL-MONITOR	AC
2022-06-01 10:59:32	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	1.1.1.1	8 (Echo Request)	0 (No Code) / icr		CATCH-ALL	AC
2022-06-01 10:59:32	Intrusion	Pass	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	1.1.1.1	8 (Echo Request)	0 (No Code) / icr		CATCH-ALL	AC
2022-06-01 10:59:32	Intrusion	Pass	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	1.1.1.1	8 (Echo Request)	0 (No Code) / icr		CATCH-ALL	AC
2022-06-01 10:59:29	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	52.139.154.55	53427 / tcp	443 (https) / tcp	NBC News	CATCH-ALL, URL-MONITOR	AC
2022-06-01 10:59:29	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	52.139.154.55	53426 / tcp	443 (https) / tcp	NBC News	CATCH-ALL, URL-MONITOR	AC
2022-06-01 10:59:25	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	13.107.246.254	53425 / tcp	443 (https) / tcp	Bing	URL-MONITOR, CATCH-ALL	AC
2022-06-01 10:59:25	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	117.18.232.200	53424 / tcp	443 (https) / tcp	Bing	CATCH-ALL	AC
2022-06-01 10:59:25	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	210.57.94.192	53423 / tcp	443 (https) / tcp	Office 365	CATCH-ALL, URL-MONITOR	AC
2022-06-01 10:59:23	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	40.90.184.73	53422 / tcp	443 (https) / tcp	Microsoft	URL-MONITOR, CATCH-ALL	AC

参考：ユーザ・グループベースの ACP ルール設定

- Policies > Access Control > Access Control

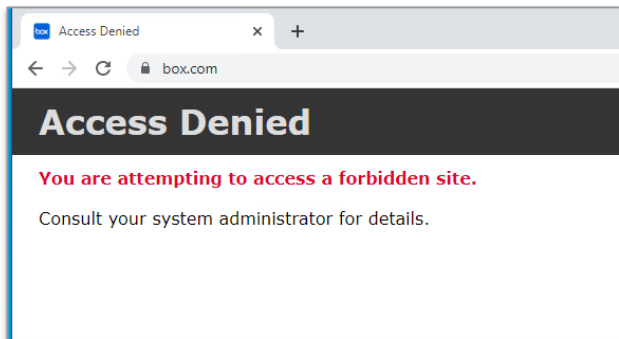


- ① HTTP Responses を選択
- ② Block Response Page で System-provided を選択
※Block ページの指定
- ③ Add Rule をクリック
- ④ 任意のルール名を入力
- ⑤ Action を Block に設定
- ⑥ Users タブを選択し、Available Realms で AD01 を選択
- ⑦ Available Users でグループ名の Sales を選択し Add to Rule をクリック

参考：ユーザ・グループベースの ACP ルール設定

- 接続テスト & Monitoring Events

Sales グループに属する Taro Yamada のアクセス



- Unified Events

Firepower Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin

🔍 Action block × × × Refresh

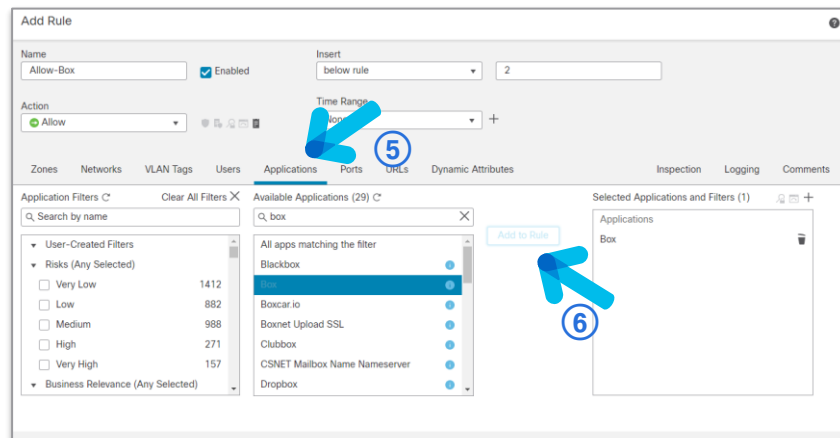
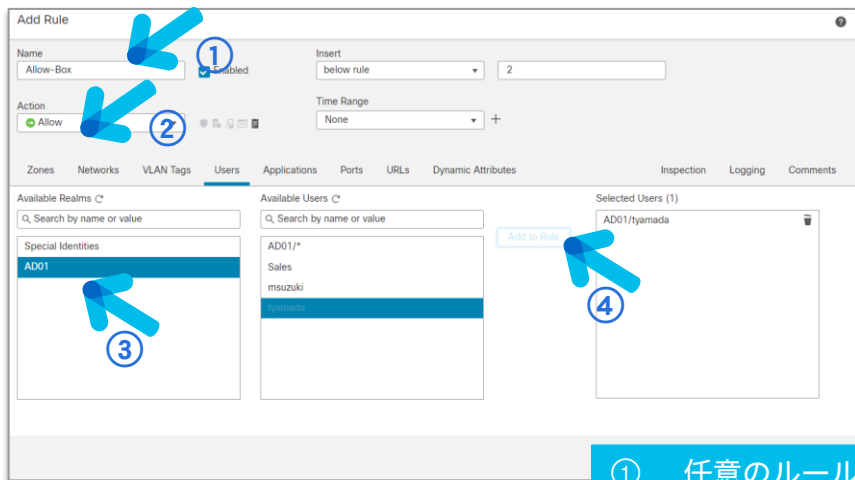
🕒 Showing all 3 events (🔍 3) ⏴ ⏵ 2022-06-01 11:04:49 JST → 2022-06-01 12:04:49 JST 1h 🟢 Go Live

🗑️	Time	Event Type	Action	Source User	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Ac
>	2022-06-01 12:02:50	🔗 Connection	🛑 Block	taro.yamada (AD01 tyamada, LDAP)	192.168.1.101	107.152.24.197	51345 / tcp	443 (https) / tcp	Box	Block-Box	AC
>	2022-06-01 12:02:49	🔗 Connection	🛑 Block	taro.yamada (AD01 tyamada, LDAP)	192.168.1.101	107.152.24.197	51344 / tcp	443 (https) / tcp	Box	Block-Box	AC
>	2022-06-01 11:48:58	🔗 Connection	🛑 Block	taro.yamada (AD01 tyamada, LDAP)	192.168.1.101	103.116.4.197	51302 / tcp	443 (https) / tcp	Box	Block-Box	AC

参考：ユーザ・グループベースの ACP ルール設定

- Sales グループでは Block だが Taro Yamada のみ例外設定追加

Policies > Access Control > Access Control > ACP-1 編集 > Add Rule

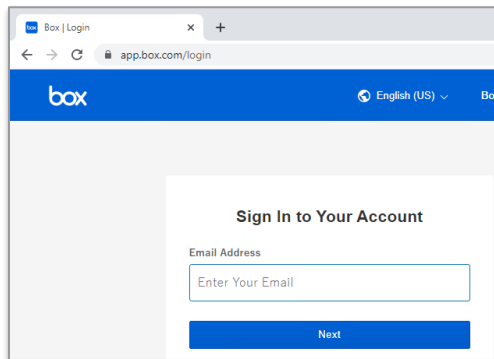


- ① 任意のルール名を入力
- ② Action で Allow を選択
- ③ Users タブに移動し、Available Realms で AD01 を選択
- ④ Available Users で tyamada を選択し、Add to Rule をクリック
- ⑤ Applications タブを選択
- ⑥ Available Applications で Box を検索して選択し、Add to Rule をクリック

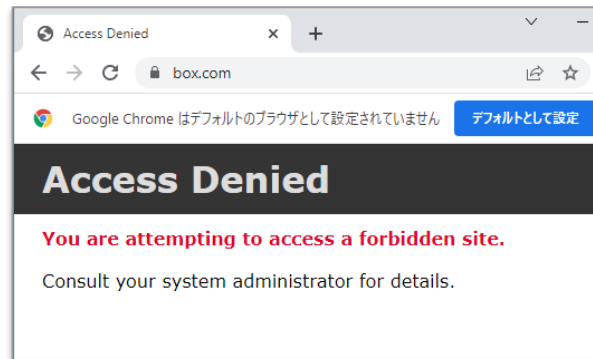
参考：ユーザ・グループベースの ACP ルール設定

・ 接続テスト & Monitoring Events

Sales グループに属する Taro Yamada のアクセス



Sales グループに属する Mika Suzuki のアクセス



・ Unified Events

Time	Event Type	Action	Source User	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule
2022-06-01 12:59:38	Connection	Block	mika suzuki (AD01\msuzuki, LDAP)	192.168.1.101	107.152.24.201	60907 / tcp	443 (https) / tcp	Box	Block-Box
2022-06-01 12:59:37	Connection	Block	mika suzuki (AD01\msuzuki, LDAP)	192.168.1.101	107.152.24.201	60905 / tcp	443 (https) / tcp	Box	Block-Box
2022-06-01 12:59:37	Connection	Block	mika suzuki (AD01\msuzuki, LDAP)	192.168.1.101	107.152.24.201	60904 / tcp	443 (https) / tcp	Box	Block-Box
2022-06-01 12:59:03	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	103.116.4.201	60839 / tcp	443 (https) / tcp	Box	Allow-Box
2022-06-01 12:58:58	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	104.16.74.20	60828 / tcp	443 (https) / tcp	Box	Allow-Box
2022-06-01 12:58:57	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	103.116.4.201	60826 / tcp	443 (https) / tcp	Box	Allow-Box
2022-06-01 12:58:57	Connection	Allow	taro yamada (AD01\tyamada, LDAP)	192.168.1.101	143.204.86.67	60825 / tcp	443 (https) / tcp	Box	Allow-Box

Monitoring Events

- Overview > switch dashboard > Access Controlled User Statistics

Firepower Management Center
Overview / Dashboards / Dashboard

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 📢 ⚙️ ? admin ▾

Reporting

Access Controlled User Statistics [\[switch dashboard\]](#)

Provides traffic and intrusion event statistics by user

Connections × Intrusion Events VPN +

Show the Last: ⌵ ||

[Add Widgets](#)

Allowed Connections by User

Username	Allowed Connections
mika suzuki (AD01\msuzuki, LDAP)	338
taro yamada (AD01\tyamada, LDAP)	119

Last updated less than a minute ago

Unique Users over Time

Last updated less than a minute ago

Traffic by User

Username	Total Bytes (KB)
mika suzuki (AD01\msuzuki, LDAP)	21,072.87
taro yamada (AD01\tyamada, LDAP)	922.12

Last updated less than a minute ago

Denied Connections by User

Username	Denied Connections
mika suzuki (AD01\msuzuki, LDAP)	3

Last updated less than a minute ago

13. AnyConnect VPN 接続の設定

FTD におけるリモートアクセス VPN

- ASA と同様に AnyConnect Client を利用したリモートアクセス VPN をサポート (TLS/DTLS, および IKEv2)
- FTD 7.0 (FMC 利用) で新たにサポートされた機能は以下の通り
 - Dynamic Access Policy (DAP)
 - AnyConnect カスタムアトリビュート
 - Per App VPN for mobile device, Dynamic Split-Tunneling, AnyConnect Defer Update
 - SAML 認可 (SAML 認証は FTD 6.7 より利用可)
 - ローカルユーザ認証
 - マルチ証明書認証
 - リモートアクセス VPN ロードバランシング

詳細は [リリースノート](#) を参照

参考) FTD7.0 (FMC 利用) でサポートされていない機能

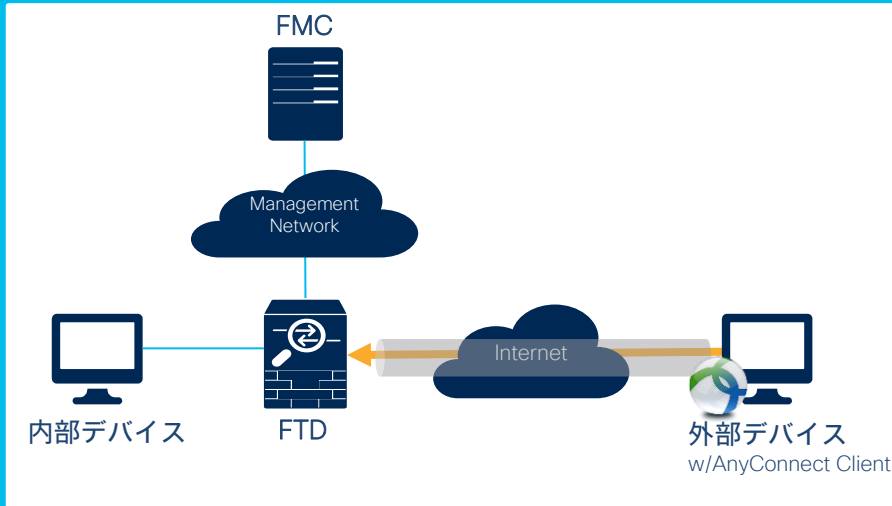
- Clientless VPN
- AnyConnect VPN SAML external browser (FTD 7.1 で利用可)
- AnyConnect customization
- AnyConnect scripts
- AnyConnect localization
- SCEP proxy
- WSA integration
- TACACS, Kerberos

本セットアップガイドでの設定条件

- VPN フルトンネル接続
- SSL (TLS/DTLS) での接続
- VPN プールアドレスは内部ネットワークアドレス (192.168.1.0/24) と同じネットワークで定義
- Local DB を作成して Local 認証を実施
 - ※12章で作成した AD レルムを利用することも可能だが、今回は 7.0 の新機能である Local 認証をテストする
- 自己証明書を作成・使用
 - Wizard での VPN ポリシー設定で ID Certificate の指定が必要なため
- VPN 通信にも Intrusion Policy、および File Policy を適用

FMC での設定ステップ

1. AnyConnect ライセンスの適用
2. AnyConnect Client のインポート
3. VPN Pool の設定
4. ID Certificate の設定
5. Local DB の設定
6. Wizard を使用したリモートアクセス VPN ポリシーの設定
7. リモートアクセス用の ACP ルール設定
8. リモートアクセス用の NAT 除外ルール設定
9. FTD への設定の Deploy
10. 端末からの接続テスト



FTD における AnyConnect ライセンス

- FTD リモートアクセス VPN 利用にあたり、以下のいずれかのスマートライセンストークンが必要
 - AnyConnect VPN-only
 - AnyConnect Plus
 - AnyConnect Apex
- ライセンスが適用されていない限りリモートアクセス VPN の設定の FTD へのデプロイは不可

※スマートライセンス適用方法については Vol.1 「4. スマートライセンスの適用」の章を参照

AnyConnect ライセンスの適用

- 利用する FTD デバイスへのライセンスのアサイン

Devices > Device Management > FTDv01 の Edit > Device タブ

FTDv01
Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP

General License System

Name: FTDv01
Transfer Packets: Yes

Performance Tier : FTDv - Variable
Base: Yes
Export-Controlled Features: Yes
Malware: Yes

Model:
Serial:
Time:
Time Zone

License

License Types
Performance Tier: FTDv - Variable

Base:
Export-Controlled Features:
Malware:
Threat:
URL Filtering:
AnyConnect Apex:
AnyConnect Plus:
AnyConnect VPN Only:

If a device already has VPN Only they cannot have Apex or Plus.
If a device has Apex or Plus it cannot have VPN Only

Cancel Save

① License の Edit ボタンをクリック
② 所有する AnyConnect ライセンスを選択
③ “Save” をクリック

AnyConnect Client のインポート

- Software Download サイトより AnyConnect Client ソフトウェアをダウンロード
 - <https://software.cisco.com/download/home>
 - AnyConnect Headend Deployment Package を選択
 - anyconnect-win-4.10.XXXX-webdeploy-k9.pkg

The screenshot shows the Cisco Software Download page for 'AnyConnect Secure Mobility Client v4.x'. The page includes a search bar, a navigation menu with 'Latest Release' selected, and a product card for 'AnyConnect Secure Mobility Client v4.x' with a release date of 4.10.05095. A warning banner indicates that AnyConnect 4.10 is available to customers with active AnyConnect Apex, Plus or VPN Only term/contracts. Below this, a table lists file information for the VPN and DART Pre-Deployment DEB Package (Linux 64-bit) and the Linux pre-deploy-deb-k9.tar.gz package.

File Information	Release Date	Size
AnyConnect VPN and DART Pre-Deployment DEB Package (Linux 64-bit)	15-Apr-2022	7.03 MB
anyconnect-linux64-4.10.05095-predeploy-deb-k9.tar.gz		

AnyConnect Client のインポート

- ダウンロードしたパッケージファイルの FMC へのインポート
Objects > Object Management > VPN > AnyConnect File

The screenshot shows the Cisco Firepower Management Center interface. The left sidebar contains a navigation menu with 'VPN' expanded and 'AnyConnect File' selected. The main content area displays the 'AnyConnect File' configuration page, which includes a table with columns for Name, Value, and Type. A table with no records is shown. A modal dialog titled 'Add AnyConnect File' is open, containing fields for Name, File Name, File Type, and Description. The 'File Type' dropdown is set to 'AnyConnect Client Image'. The 'Save' button is highlighted.

- ① Add AnyConnect File をクリック
- ② Browse をクリックしてダウンロードしたパッケージファイルを選択
- ③ AnyConnect Client Image を選択
- ④ Save をクリック

VPN Pool アドレスの設定

- Objects > Object Management > Address Pools > IPv4 Pools

① Add IPv4 Pools をクリック

② 任意のプール名を入力

③ プールする IP アドレスの範囲を入力

④ サブネットマスクを入力

⑤ Save をクリック

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

ID Certificate の設定

・ 自己証明書の生成と登録

Objects > Object Management > PKI > Cert Enrollment

- ① Add Cert Enrollment をクリック
- ② 任意の証明書名を入力
- ③ CA Information タブを選択し、Enrollment Type で Self Signed Certificateを選択
- ④ Certificate Parameters タブを選択し、パラメータを入力 (CNはマスト)
- ⑤ Key タブを選択し必要に応じてKeyを生成 (今回は Default-RSA-Key を利用)
- ⑥ Saveをクリック

The screenshot displays the Firepower Management Center interface for creating a new Cert Enrollment object. The interface is divided into several sections, with blue arrows and numbered callouts (1-6) indicating the required steps:

- Step 1:** The "Add Cert Enrollment" button in the top right corner of the main content area is highlighted with a red box and a blue arrow.
- Step 2:** The "Name*" input field in the "Add Cert Enrollment" dialog is highlighted with a red box and a blue arrow.
- Step 3:** The "CA Information" tab in the "Add Cert Enrollment" dialog is highlighted with a red box and a blue arrow. The "Enrollment Type" dropdown is set to "Self Signed Certificate".
- Step 4:** The "Certificate Parameters" tab in the "Add Cert Enrollment" dialog is highlighted with a red box and a blue arrow. The "Common Name (CN)" field is highlighted with a red box and a blue arrow.
- Step 5:** The "Key" tab in the "Add Cert Enrollment" dialog is highlighted with a red box and a blue arrow. The "Key Name" dropdown is set to "<Default-RSA-Key>".
- Step 6:** The "Save" button at the bottom right of the "Add Cert Enrollment" dialog is highlighted with a red box and a blue arrow.

The left sidebar shows the navigation menu with "PKI" and "Cert Enrollment" highlighted. The main content area shows the "Cert Enrollment" page with a description: "A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates in your Private Key Infrastructure (PKI)."

ID Certificate の設定

- FTD デバイスへの ID Certificate の登録
Devices > Certificates

- ① Add をクリック
- ② 任意のデバイス名を入力
- ③ 作成した FTDv01-ID-Certificate を選択
- ④ Add をクリック

The screenshot shows the Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Devices' tab is active, and the 'Certificates' sub-tab is selected. A table lists certificates with columns for Name, Domain, Enrollment Type, and Status. An 'Add' button is visible in the top right corner of the table area.

An 'Add New Certificate' dialog box is open, showing the following fields and values:

- Device*: FTDv01
- Cert Enrollment*: FTDv01-ID-Certificate
- Cert Enrollment Details:
 - Name: FTDv01-ID-Certificate
 - Enrollment Type: Self-Signed
 - Enrollment URL: N/A

The 'Add' button at the bottom right of the dialog is highlighted. A blue arrow points from the 'Add' button in the main interface to the 'Add' button in the dialog.

A second screenshot shows the 'Certificates' table after the certificate has been added. The table now includes a row for 'FTDv01-ID-Certificate' with a magnifying glass icon next to the 'ID' column. A blue callout box points to this icon with the text: '登録されると虫眼鏡アイコンとなる' (When registered, it becomes a magnifying glass icon).

Local DB の設定

- ・今回認証には Local DB を利用するため、Local DB の設定を実施
System > Integration > Realms

The screenshot shows the 'Add New Realm' dialog box in the Cisco Firepower Management Center. The dialog is titled 'Add New Realm' and has a close button (X) in the top right corner. It contains the following fields and sections:

- Name***: A text input field containing 'Local-DB'. A blue arrow labeled '2' points to this field.
- Description**: An empty text input field. A blue arrow labeled '1' points to this field.
- Type**: A dropdown menu showing 'LOCAL'. A blue arrow labeled '3' points to this dropdown.
- Local User Configuration**: A section containing:
 - Username**: A text input field containing 'ngfw-user1'. A blue arrow labeled '4' points to this field.
 - Password**: A password input field. A blue arrow labeled '4' points to this field.
 - Confirm Password**: A password input field. A blue arrow labeled '4' points to this field.
- Add another local user**: A button with a blue arrow labeled '5' pointing to it.
- Buttons**: 'Cancel' and 'Save' buttons at the bottom. A blue arrow labeled '6' points to the 'Save' button.

In the background, the 'Realms' page is visible, showing a table with 'Compare Realms' and 'Add Realm' buttons. A red box highlights the 'Add Realm' button, with a blue arrow labeled '1' pointing to it.

- ① Add Realm をクリック
- ② 任意のレルム名を入力
- ③ Type で LOCAL を選択
- ④ Local User Configuration でユーザ ID、パスワードを登録
- ⑤ 追加のユーザを登録する場合には Add another local user をクリックして追加 (ユーザは Local Realm 作成後にも追加可能)
- ⑥ Save をクリック

Wizard を使用した RAVPN ポリシー設定

- ・ リモートアクセス VPN のポリシーを設定
Devices > VPN > Remote Access
- ・ VPN プロトコルの選択、および VPN 終端デバイスの選択

Firepower Management Center
Devices / VPN / Remote Access

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy 🔍 ⚙️ ⓘ admin ▾

Firepower Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy 🔍 ⚙️ ⓘ admin ▾

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*
RAVPN

Description:

VPN Protocols:

SSL
 IPsec-IKEV2

Targeted Devices

Available Devices

FTDv01

Selected Devices

FTDv01

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.

AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

1 Add をクリック

2 任意のポリシー名を入力

3 VPN Protocols の選択 (今回は SSL のテストのため、IPsec-IKEV2 のチェックを外す)

4 Target Devices で FTDv01 を選択し Add をクリック

5 Next をクリック

Cancel Back Next

Wizard を使用した RAVPN ポリシー設定

・ 認証方式の選択

Firepower Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy 🔍 ⚙️ ⓘ admin ▾

Remote Access VPN Policy Wizard

① Policy Assignment — ② **Connection Profile** — ③ AnyConnect — ④ Access & Certificate — ⑤ Summary

Remote User — AnyConnect Client — Internet — Outside — VPN Device — Inside — Corporate Resources

AAA

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*

① This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for connections.

Authentication Method:

Authentication Server:*
(LOCAL or Realm or RADIUS)

Local Realm:*

① Connection Profile Name は VPN ポリシー名と同じ名前が自動入力される
② Authentication Method で AAA Only を選択
③ Authentication Server で LOCAL を選択
④ Local Realm は作成済みの LOCAL 認証用 Realm 名を選択

Wizard を使用した RAVPN ポリシー設定

• VPN プールアドレスの指定

Firepower Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin ▼

Remote Access VPN Policy Wizard

① Policy Assignment — ② Connection Profile — ③ AnyConnect — ④ Access & Certificate — ⑤ Summary

(LOCAL or realm or RADIUS)

Local Realm:* Local-DB +

Authorization Server: +
(Realm or RADIUS)

Accounting Server: +
(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: VPN-Pool

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when connection is established. Select or create a Group Policy object.

Group Policy:* DfltGrpPolicy +
[Edit Group Policy](#)

Address Pools

Available IPv4 Pools +

Q Search

VPN-Pool

Add

Selected IPv4 Pools

VPN-Pool

Cancel OK

- ① Client Address Assignment で Use IP Address Pools を選択
- ② IPv4 Address Pools の Edit をクリック
- ③ 作成済みのプール名を選択して Add をクリック
- ④ OK をクリック

Wizard を使用した RAVPN ポリシー設定

• Group Policy の作成

Firepower Management Center
Devices / VPN / Setup Wizard

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Local Realm*: Local-DB +

Authorization Server: +
(Realm or RADIUS)

Accounting Server: +
(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: VPN-Pool

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a connection is established. Select or create a Group Policy object.

Group Policy*: DfltGrpPolicy +

Edit Group Policy

Add Group Policy

Name*: RAVPN-GP

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

1 新規 Group Policy を作成。Group Policy で追加をクリック

2 任意の Group Policy 名を入力

3 VPN Protocols で SSL のみチェック

Cancel Back Next

Wizard を使用した RAVPN ポリシー設定

・ Group Policy での DNS サーバ設定

Add Group Policy

Name: *
RAVPN-GP

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Primary DNS Server: +

Secondary DNS Server: -

Primary WINS Server: +

Secondary WINS Server: +

DHCP Network Scope: +

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Cancel Save

New Network Object

Name
DNS_Server1

Description

Network
 Host Range Network FQDN

192.168.1.11

Allow Overrides

Cancel Save

Add Group Policy

Name: *
RAVPN-GP

Description:

General AnyConnect Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Primary DNS Server: +
DNS_Server1

Secondary DNS Server: -

Primary WINS Server: +

Secondary WINS Server: +

DHCP Network Scope: +

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Cancel Save

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy: *
RAVPN-GP

Edit Group Policy

Cancel Back Next

前ページの続き

- ① DNS/WINS を選択
- ② Primary DNS Server の Add をクリック
- ③ 任意の DNS サーバ名を入力
- ④ Host を選択し DNS サーバアドレスを入力
- ⑤ Save をクリック
- ⑥ 作成した DNS サーバ名が選択されていることを確認して Save をクリック
- ⑦ Wizard に戻り、作成した Group Policy 名が選択されているのを確認して Next をクリック

Wizard を使用した RAVPN ポリシー設定

- AnyConnect Client Image の指定

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Remote User — AnyConnect Client — Internet — Outside — VPN Device — Inside — Corporate Resources

AAA

AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	anyconnect-win-4.10.05095-we...	anyconnect-win-4.10.05095-webdeploy-k9...	Windows

Cancel Back Next

- ① 先に FMC にインポート済の AnyConnect Client File を選択
- ② Next をクリック

Wizard を使用した RAVPN ポリシー設定

- VPN アクセスインタフェースの指定、および ID 証明書の指定

Firepower Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — **4 Access & Certificate** — 5 Summary

Remote User — AnyConnect Client — Internet — Outside — VPN Device — Inside — Corporate Resources

AAA

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

⚠️ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

① Network Interface for Incoming VPN Access で Outside_Zone を選擇
② Device Certificates で FTDv01-ID-Certificate に割り当済みの証明書を選擇
③ Next をクリック

Cancel Back **Next**

Wizard を使用した RAVPN ポリシー設定

- Wizard 設定内容の確認

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: RAVPN
Device Targets: FTDN01
Connection Profile: RAVPN
Connection Alias: RAVPN

AAA:

Authentication Method: AAA-Only
Authentication Server: LDAP-08 (Local)
Authorization Server: -
Accounting Server: -

Address Assignment:

Address from AAA: -
DHCP Servers: -
Address Pools (IPv4): VPN-Pool
Address Pools (IPv6): -

Group Policy: RAVPN-GP

AnyConnect Images: anyconnect-win-4.10.05005-webkitdeploy-k9.pkg
Interface Objects: Outside_Zone

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update
An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.
- DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using HostControl Policy on the targeted devices.
- Port Configuration
SSL will be enabled on port 443. Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

1

Cancel Back Finish

- 1 Wizard で設定された内容を確認し、問題なければ Finish をクリック
- 2 新しい接続プロファイルが作成されていることを確認
- 3 SAVE をクリック

Firepower Management Center

Overview Analysis Policies Devices Objects AMP Intelligence

RAVPN

Enter Description

Local Realm: Local-DB Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

Name	Authentication	Group Policy
DefaultVEBVPNGroup	Authentication: None Authorization: None	DfltGrpPolicy
RAVPN	Authentication: LOCAL Authorization: None Accounting: None	RAVPN-GP

2

Save Cancel

リモートアクセス用 ACP ルール設定

- RAVPN アクセス時にも Intrusion & File ポリシーを適用する ACP ルールを追加

Policies > Access Control > Access Control

- ① ACP-1 の Edit をクリック
- ② Add Rule をクリック


Firepower Management Center
Policies / Access Control / Access Control

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin ▾

Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export

New Policy

Access Control Policy	Domain	Status	Last Modified	
ACP-1	Global	Targeting 1 devices Up-to-date on all targeted devices	2022-05-18 11:51:16 Modified by "Firepower System"	

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin ▾

ACP-1

Enter Description

Show Warnings Analyze Hit Counts Save Cancel




Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging ⚠️ Advanced

Prefilter Policy: Default Prefilter Policy SSL Policy: SSL-POLICY Identity Policy: None

Filter by Device 🔍 Search Rules

Show Rule Conflicts + Add Category **+ Add Rule**

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	
Mandatory - ACP-1 (-)															
There are no rules in this section. Add Rule or Add Category															
Default - ACP-1 (1-3)															
1	TIME-BASED (Disabled)	Any	Any	OFFICE	Any	Any	Any	Any	Any	Any	Any	Any	Any	Block	
2	URL-MONITOR	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any (Except Unci	Any	Any	Monitor	
3	CATCH-ALL	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	

リモートアクセス用 ACP ルール設定

- Zones, Networks (VPN プールアドレスの Network Object 作成)

Add Rule

Name: RAVPN-Access [Enabled]

Insert: above rule | 1

Action: Allow

Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Available Zones: Search by name, Inside_Zone, Outside_Zone

Source Zones (1): Outside_Zone

Destination Zones (0): any

Add to Source

Add Rule

Name: RAVPN-Access [Enabled]

Insert: above rule | 1

Action: Allow

Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs Dynamic Attributes Inspection Logging Comments

Available Networks: Search by name or value, 192.168.1.0_inside_hosts, any, any-ipv4, any-ipv6, asa_default_gw, DNS_Server1, in_host1, in_mapped_host1

Source Networks (0): any

Destination Networks (0): any

Add Object

New Network Object

Name: VPN-Pool-IPs

Description:

Network: Host Range Network FQDN

192.168.1.201-192.168.1.210

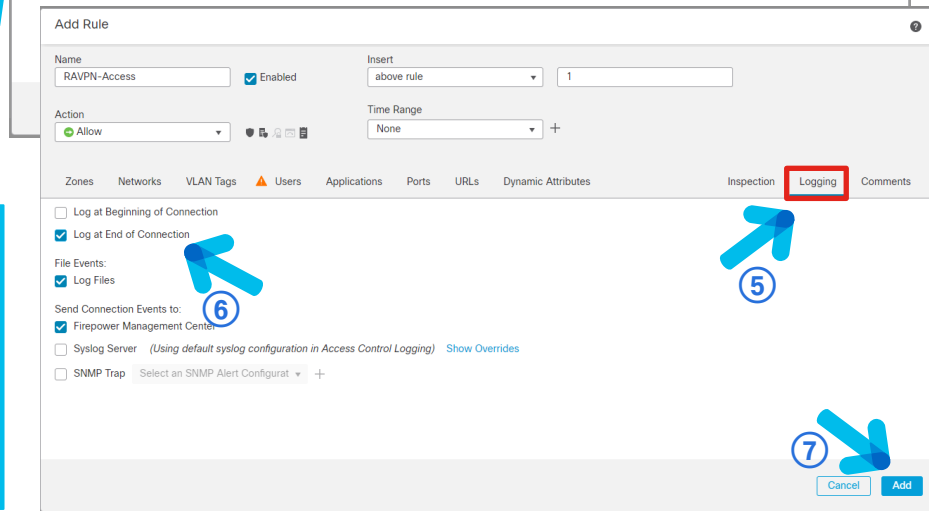
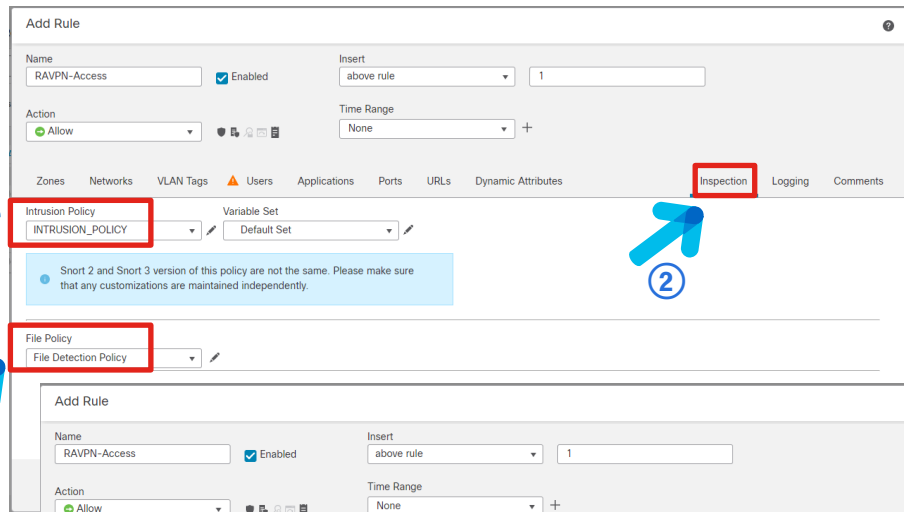
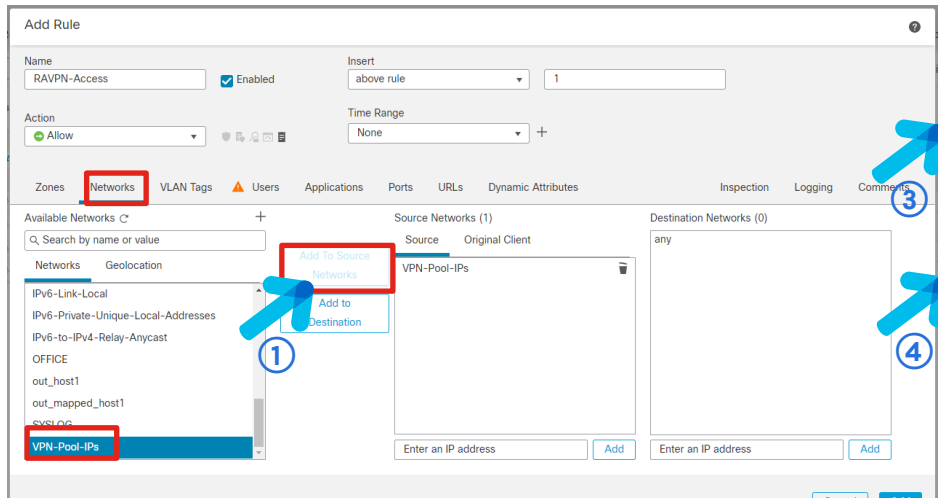
Allow Overrides

Cancel Save

- ① 任意のルール名を入力
- ② Insert で above rule を選択し、1 に設定
- ③ Action は Allow を選択
- ④ Zones タブで Available Zones から Outside_Zone を選択し、Add to Source をクリック
- ⑤ Networks タブを選択
- ⑥ Available Networks の追加を選択し、Add Object を選択
- ⑦ New Network Object で VPN プールオブジェクトを作成。任意の名前を入力
- ⑧ Network で Range を指定し、設定した VPN プールと同じアドレス範囲を入力

リモートアクセス用 ACP ルール設定

- Networks, Inspection, Logging



- ① 作成したオブジェクトを選択して Add to Source Networks をクリック
- ② Inspection タブをクリック
- ③ Intrusion Policy で作成済の INTRUSION_POLICY を選択
- ④ File Policy で作成済の File Detection Policy を選択
- ⑤ Logging タブを選択
- ⑥ Log at End of Connection を選択
- ⑦ Add をクリック

リモートアクセス用 ACP ルール設定

- ACP ルールの保存

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy admin

ACP-1

You have unsaved changes Show Warnings Analyze Hit Counts **Save** Cancel

Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging **Advanced**

Prefilter Policy: Default Prefilter Policy SSL Policy: SSL-POLICY Identity Policy: None

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	
Mandatory - ACP-1 (-)															
There are no rules in this section. Add Rule or Add Category															
Default - ACP-1 (1-4)															
1	RAVPN-Access	Outside_Zone	Any	VPN-Pool-IPs	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	
2	RAVPN-Access (Disabled)	Any	Any	OFFICE	Any	Any	Any	Any	Any	Any	Any	Any	Any	Block	
3	URL-MONITOR	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any (Except Unc...	Any	Any	Monitor	
4	CATCH-ALL	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	

① Save をクリックして設定を保存

リモートアクセス用の NAT 除外設定

- RAVPN 接続クライアントからの通信が FTD に戻るときに NAT されないように、RAVPN 通信用の NAT 除外ルールを追加

Devices > NAT

- ① 既存の NAT ポリシーの Edit をクリック
- ② Add Rule をクリック

Firepower Management Center
Devices / NAT

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin ▾

New Policy

NAT Policy	Device Type	Status
FTDv01_NAT_Policy For FTDv01	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

FTDv01_NAT_Policy
For FTDv01

Show Warnings Save Cancel

Policy Assignments (1)

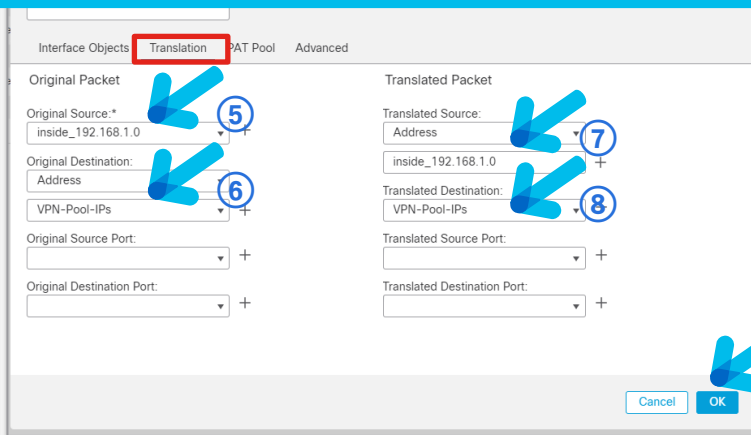
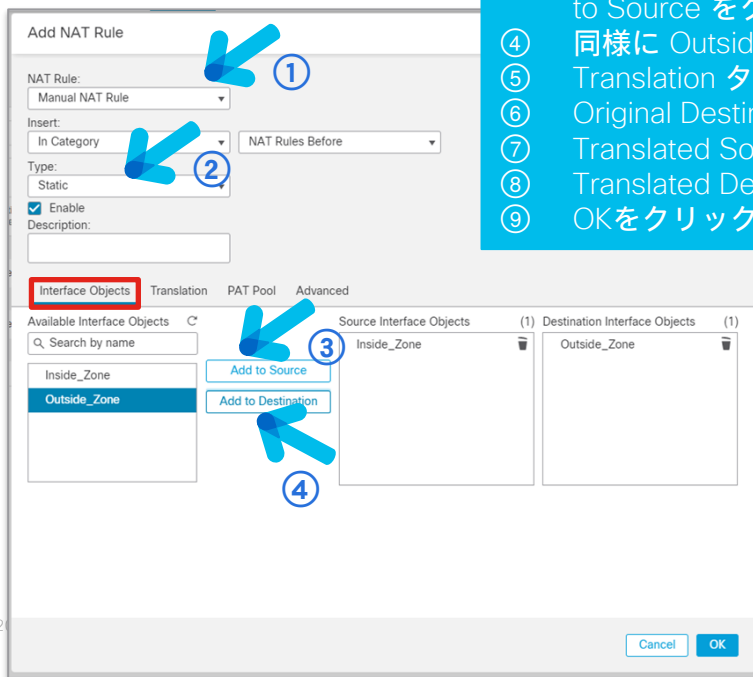
Filter by Device Filter Rules

#	Direction	Type	Original Packet			Translated Packet				Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	
1	↔	Static	Inside_Zone	Outside_Zone	in_host1	out_host1	in_mapped_host1	out_mapped_host1	Dns:false	🗑️

リモートアクセス用の NAT 除外設定

- Interface Objects, Translation

- ① Manual NAT Rule を選択
- ② Type で Static を選択
- ③ Interface Objects タブで、Available Interface Objects から Inside_Zone を選択して Add to Source をクリック
- ④ 同様に Outside_Zone を選択して Add to Destination をクリック
- ⑤ Translation タブに移動し、Original Source で Inside のネットワークオブジェクトを選択
- ⑥ Original Destination で Address を選択し VPN-Pool-IPs を選択
- ⑦ Translated Source で Address を選択して Inside のネットワークオブジェクトを選択
- ⑧ Translated Destination で VPN-Pool-IPs を選択
- ⑨ OKをクリック



リモートアクセス用の NAT 除外設定

- NAT ルールの保存と VPN 設定の FTD への展開

- ① 右上の Save ボタンをクリックして設定を保存
- ② Deploy を選択し、FTDv01 を選択
- ③ Deploy ボタンをクリック

FTDv01_NAT_Policy
For FTDv01

You have unsaved changes [Show Warnings](#) [Save](#) [Cancel](#)

Policy Assignments (1)

Rules

Filter by Device Filter Rules [Add Rule](#)

#	Direction	Type	Original Packet		Translated Packet					Options		
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations			Translated Services
NAT Rules Before												
1	↔	Static	Inside_Zone	Outside_Zone	in_host1	out_host1		in_mapped_host1	out_mapped_host1		Dns:false	🗑️
2	↔	Static	Inside_Zone	Outside_Zone	inside_192.168.1.0	VPN-Pool-IPs		inside_192.168.1.0	VPN-Pool-IPs		Dns:false	🗑️
Auto NAT Rules												
#	✖	Dyna...	Inside_Zone	Outside_Zone	192.168.1.0_inside_hosts			Interface			Dns:false	🗑️
NAT Rules After												

Firepower Management Center
Deploy / Deployment

Overview Analysis Policies Devices Objects AMP Intelligence

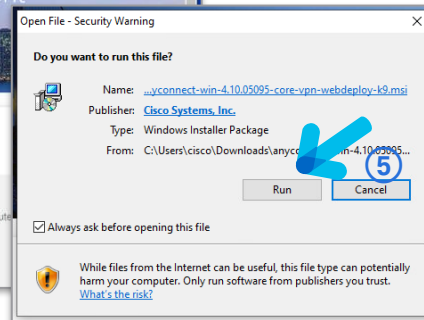
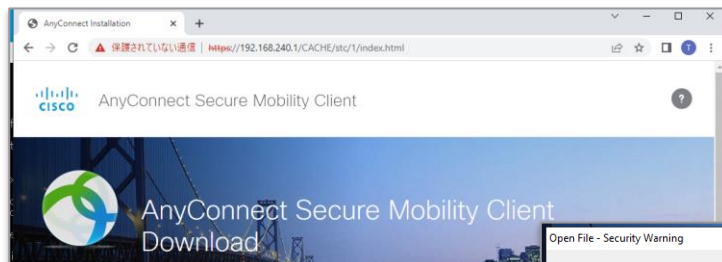
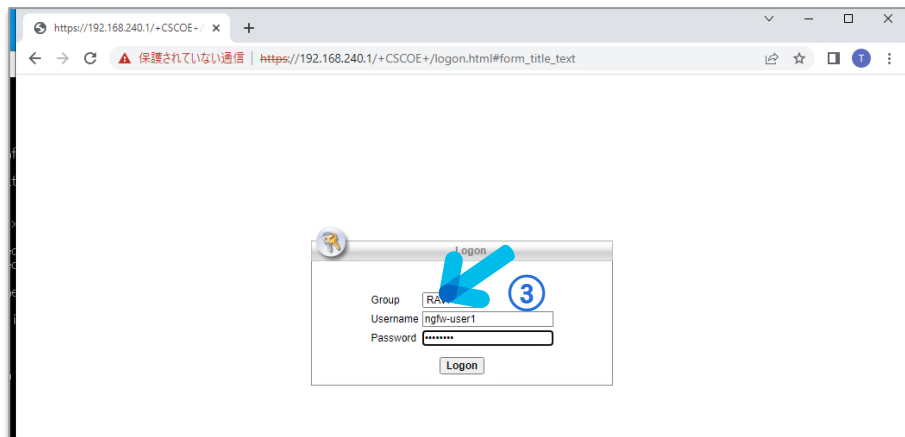
[Deploy](#) 🔍 ⚙️ ? admin ▼

1 device selected
Deploy time: Estimate [Deploy](#)

② Search using device name, user name, type, group or status

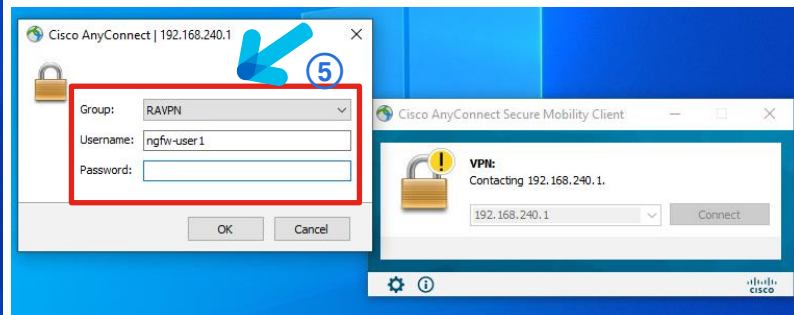
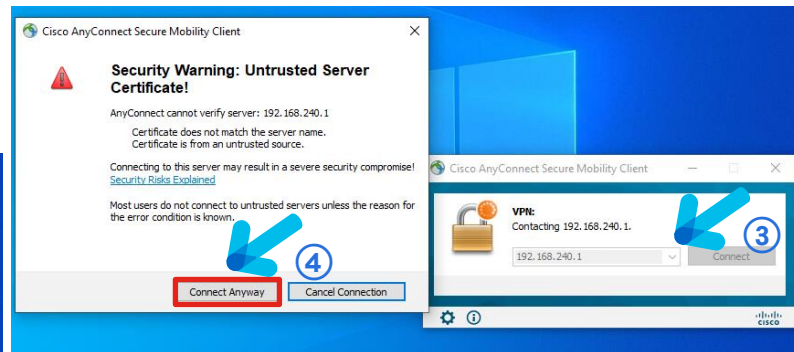
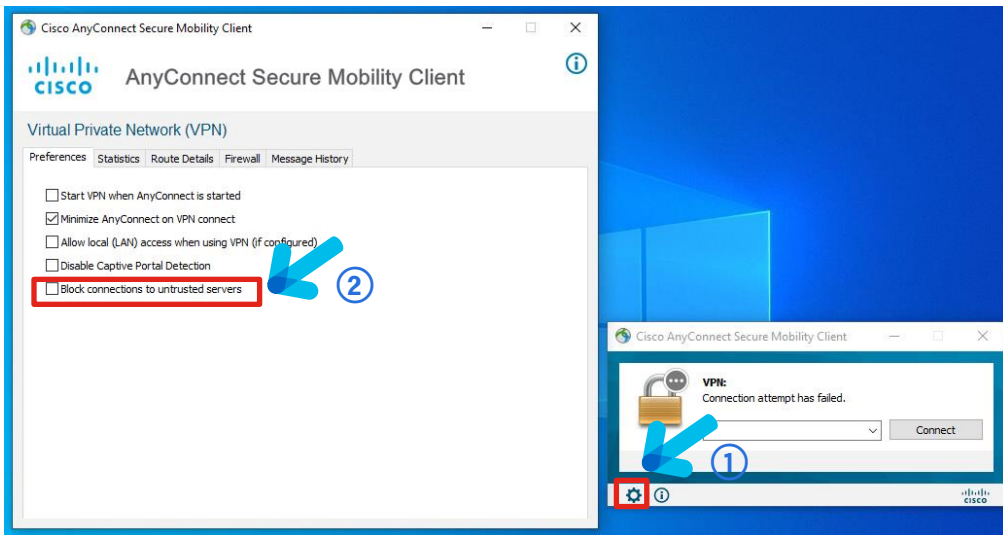
Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
> <input checked="" type="checkbox"/> FTDv01	Admin		FTD		May 24, 2022 3:45 PM	🗑️	Pending

接続テスト

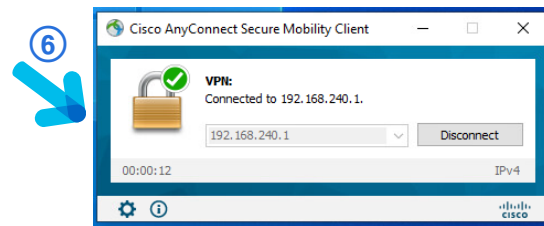


- ① 今回はテスト接続のため test PC-2 のブラウザで https://192.168.240.1 へアクセス
- ② プライバシー接続のエラーが表示されるが、今回はテスト接続なのでこれを無視し、そのまま「192.168.240.1 にアクセスする」をクリック (以降、類似エラーは無視することとする)
- ③ Group で RAVPN を選択し、Local DB で設定したユーザ名/パスワードを入力
- ④ Download for Windows をクリックして AnyConnect Client をダウンロード
- ⑤ test PC-2 にて AnyConnect Client をインストール

接続テスト



- ① AnyConnect Client を起動しギアマークをクリック
- ② Preferences で Block connections to untrusted servers のチェックを外す
- ③ AnyConnect Client で 192.168.240.1 を入力して Connect をクリック
- ④ Security Warning が表示されるが Connect Anyway をクリック
- ⑤ ユーザ名/パスワードを入力して OK をクリック
- ⑥ RAVPN 接続完了



Monitoring Events

- Overview > switch dashboard > Access Controlled User Statistics

The screenshot displays the Cisco Firepower Management Center interface. The main heading is "Access Controlled User Statistics" with a sub-heading "Provides traffic and intrusion event statistics by user". A red box highlights the "(switch dashboard)" link, and a red arrow points to a dropdown menu that lists various dashboard options, with "Access Controlled User Statistics" selected. The dashboard contains six widgets:

- Active VPN Sessions by Duration:** Shows a single entry for user "Local-DB\ngfw-user1 (LDAP)" with a session duration of 21 minutes.
- Active VPN Sessions by Device:** Shows a single entry for device "FTDv01" with a count of 1.
- VPN Users by Duration:** Shows a single entry for user "ngfw-user1" with a connection duration of 2 hours.
- Active VPN Sessions by Client Application:** Shows a single entry for "Cisco AnyConnect VPN Agent for Windows 4.10.05095" with a count of 1.
- VPN Users by Data Transferred:** Shows a single entry for user "ngfw-user1" with a total of 384,384 bytes transferred.
- VPN Users by Client Application:** Shows a single entry for "Cisco AnyConnect VPN Agent for Windows 4.10.05095" with a count of 7.

Each widget includes a "Last updated 3 minutes ago" timestamp and a refresh icon. The interface also features a navigation bar with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence, and a top right corner with a user profile for "admin".

Monitoring Events

- Analysis > Users > User Activity

Firepower Management Center
Analysis / Users / User Activity

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin ▾

[Bookmark This Page](#) | [Reporting](#) | [Dashboard](#) | [View Bookmarks](#) | [Search](#)

2022-05-11 17:57:41 - 2022-05-25 17:57:41
Static

▶ Search Constraints ([Edit Search](#) [Save Search](#))

Table View of Events Users

<input type="checkbox"/>	Time	Event	Username	Realm	Authentication Type	IP Address	Description	VPN Session Type	VPN Group Policy	VPN Connection Profile	VPN Client Public IP	VPN Client Country	VPN Client OS	VPN Client Application	VPN Connection Duration	VPN Bytes Out	VPN Bytes In	Secu. Group Tag
▼ <input type="checkbox"/>	2022-05-25 17:36:12	VPN User Login	ngfw-user1	Local-DB	VPN Authentication	192.168.1.201		AnyConnect SSL	RAVPN-GP	RAVPN	192.168.240.101		win	Cisco AnyConnect VPN Agent for Windows 4.10.05095	0	0	0	
▼ <input type="checkbox"/>	2022-05-24 17:40:45	VPN User Logoff	ngfw-user1	Local-DB	VPN Authentication	192.168.1.201	User Requested	AnyConnect SSL	RAVPN-GP	RAVPN	192.168.240.101		win	Cisco AnyConnect VPN Agent for Windows 4.10.05095	1 hour	185,733	14,464	
▼ <input type="checkbox"/>	2022-05-24 15:46:37	VPN User Login	ngfw-user1	Local-DB	VPN Authentication	192.168.1.201		AnyConnect SSL	RAVPN-GP	RAVPN	192.168.240.101		win	Cisco AnyConnect VPN Agent for Windows 4.10.05095	0	0	0	
▼ <input type="checkbox"/>	2022-05-24 15:41:21	VPN User Logoff	ngfw-user1	Local-DB	VPN Authentication	192.168.1.201	User Requested	AnyConnect SSL	RAVPN-GP	RAVPN	192.168.240.101		win	Cisco AnyConnect VPN Agent for Windows 4.10.05095	28 seconds	25,269	14,464	
▼ <input type="checkbox"/>	2022-05-24 15:40:53	VPN User Login	ngfw-user1	Local-DB	VPN Authentication	192.168.1.201		AnyConnect SSL	RAVPN-GP	RAVPN	192.168.240.101		win	Cisco AnyConnect VPN Agent for Windows 4.10.05095	0	0	0	
▼ <input type="checkbox"/>	2022-05-19 18:54:11	VPN User Logoff	ngfw-user1	Local-DB	VPN Authentication	192.168.1.201	User Requested	AnyConnect SSL	RAVPN-GP	RAVPN	192.168.240.101		win	Cisco AnyConnect VPN Agent for Windows 4.10.05095	28 minutes	103,714	40,740	
▼ <input type="checkbox"/>	2022-05-19 18:25:53	VPN User Login	ngfw-user1	Local-DB	VPN Authentication	192.168.1.201		AnyConnect SSL	RAVPN-GP	RAVPN	192.168.240.101		win	Cisco AnyConnect VPN Agent for Windows 4.10.05095	0	0	0	

Page 1 of 1 | Displaying rows 1-7 of 7 rows

Monitoring Events

- Unified Events
 - VPN 端末 192.168.1.201 から 内部端末 192.168.1.101 への ICMP 通信を Intrusion Policy で検知

Firepower Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 ⚙️ 👤 admin ▼

🔍 Source or Destination IP 192.168.1.201 x Refresh

📌 Showing all 103 events (📄 93 📌 10) ⏏ 2022-05-25 17:06:20 JST → 2022-05-25 18:06:20 JST 1h 🔄 Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Contr
2022-05-25 17:55:07	Connection	Allow		192.168.1.201	64.104.14.184	52514 / udp	53 (domain) / ucp		RAVPN-Access	ACP-1
2022-05-25 17:55:51	Connection	Allow		192.168.1.201	192.168.1.101	8 (Echo Request)	0 (No Code) / icm		RAVPN-Access	ACP-1
2022-05-25 17:55:33	Connection	Allow		192.168.1.201	192.168.1.101	8 (Echo Request)	0 (No Code) / icm		RAVPN-Access	ACP-1
2022-05-25 17:55:15	Connection	Allow		192.168.1.201	192.168.1.101	8 (Echo Request)	0 (No Code) / icm		RAVPN-Access	ACP-1
2022-05-25 17:55:12	Intrusion	Pass		192.168.1.201	192.168.1.101	8 (Echo Request)	0 (No Code) / icm		RAVPN-Access	ACP-1

Event Type: Intrusion

Time: 2022-05-25 17:55:12

Priority: medium

Impact: Impact 2

Action: Pass

Source IP: 192.168.1.201

Destination IP: 192.168.1.101

Source Port / ICMP Type: 8 (Echo Request) / icmp

Destination Port / ICMP Code: 0 (No Code) / icmp

SSL Status: Unknown (Unknown)

Intrusion Message: PROTOCOL-ICMP Unusual PING detected (1:29456...

Classification: Information Leak

Generator: Standard Text Rule

Source User: No Authentication Required

Application Protocol: ICMP

Application Protocol Category: network protocols/services

Client Application: ICMP client

Application Risk: Medium

Business Relevance: Medium

Ingress Security Zone: Outside_Zone

Device: FTDV01

Ingress Interface: Outside

Egress Interface: Inside

Ingress Virtual Router: Global

Egress Virtual Router: Global

Intrusion Policy: INTRUSION_POLICY

Access Control Policy: ACP-1

Access Control Rule: RAVPN-Access

Network Analysis Policy: Balanced Security and Connectivity

HTTP Response Code: 0

2022-05-25 17:55:12	Intrusion	Pass		192.168.1.201	192.168.1.101	8 (Echo Request)	0 (No Code) / icm		RAVPN-Access	ACP-1
2022-05-25 17:55:00	Connection	Allow		192.168.1.201	192.168.1.101	8 (Echo Request)	0 (No Code) / icm		RAVPN-Access	ACP-1

CLI での確認

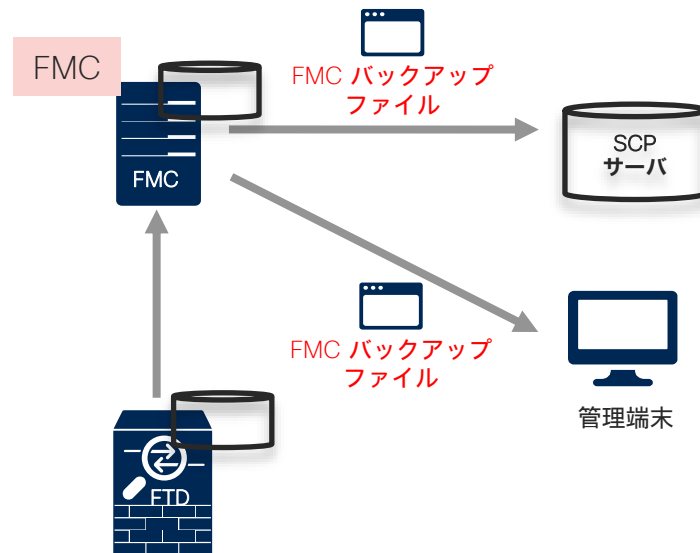
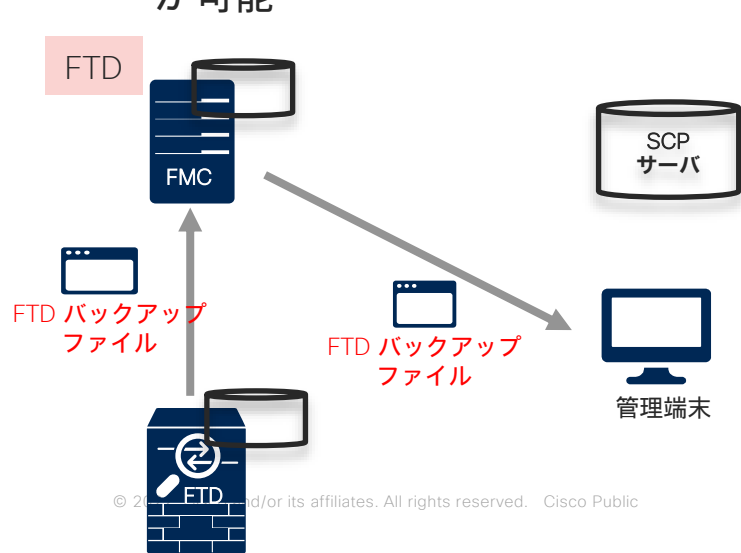
- FTDv01 上での show command – show vpn-sessiondb anyconnect

```
> show vpn-sessiondb anyconnect
Session Type: AnyConnect
Username      : ngfw-user1          Index      : 7
Assigned IP   : 192.168.1.201      Public IP  : 192.168.240.101
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx      : 14464              Bytes Rx   : 29650
Group Policy  : RAVPN-GP           Tunnel Group : RAVPN
Login Time    : 08:36:12 UTC Wed May 25 2022
Duration      : 0h:11m:30s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                VLAN       : none
Audt Sess ID  : c0a8f00100007000628dea7c
Security Grp  : none                Tunnel Zone : 0
```

14. バックアップの設定とリストアの方法

バックアップについて

- FMC, FTD とともにバックアップの取得が可能
- FTD バックアップの保存先は FTD ローカル、もしくは FMC ローカル
- FMC バックアップは FMC ローカルへのダウンロード、およびリモートサーバ (SCP) へコピー
- FMC に保存したバックアップファイルは、FMC の GUI より管理端末へダウンロードすることが可能



本章のバックアップに関する操作の流れ

- FTD デバイスのバックアップ取得
 - FTD デバイスのバックアップファイル確認
 - FMC のバックアップ取得
 - FMC のバックアップファイル確認
-
- SCP サーバは、管理ネットワークに存在している PC を利用
 - FTD, FMC とともに HA でもバックアップ取得は可能

FTD デバイスのバックアップ取得 ①

- FMC で管理している FTD デバイスのバックアップを取得

The screenshot shows the Firepower Management Center (FMC) interface. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', and 'Deploy'. The 'Backup Management' section is active, showing 'Firepower Management Backups' and 'Managed Device Backup' buttons. A table lists backup entries with columns for System Information, Date Created, File Name, VDB Version, Location, Size (MB), Configurations, Events, and TID. A blue callout box on the right provides instructions for the steps shown in the image.

① System (歯車マーク) → Backup/Restore を選択

② (FMC を新規でインストールした場合) デフォルトでスケジュールされた FMC のバックアップデータが存在していれば、その一覧が表示されている

③ Managed Device Backup をクリック

System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
<input type="checkbox"/> FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-22 11:07:20	Weekly_config_only_backup_202205222020002-2022-05-22T02-00-05.tar	build 351	Local	451	Yes	No	No
<input type="checkbox"/> FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-15 11:06:42	Weekly_config_only_backup_20220515020002-2022-05-15T02-00-05.tar	build 351	Local	318	Yes	No	No
<input type="checkbox"/> FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-08 11:06:54	Weekly_config_only_backup_20220508020002-2022-05-08T02-00-05.tar	build 351	Local	317	Yes		
<input type="checkbox"/> FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-01 11:07:01	Weekly_config_only_backup_20220501020002-2022-05-01T02-00-04.tar	build 351	Local	312	Yes		
<input type="checkbox"/> FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-04-24 11:06:47	Weekly_config_only_backup_20220424020002-2022-04-24T02-00-05.tar	build 351	Local	312	Yes		
<input type="checkbox"/> FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-04-17 11:06:58	Weekly_config_only_backup_20220417020002-2022-04-17T02-00-05.tar	build 351	Local	290	Yes		
<input type="checkbox"/> FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-04-10 11:06:37	Weekly_config_only_backup_20220410020002-2022-04-10T02-00-04.tar	build 351	Local	281	Yes		
<input type="checkbox"/> FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-04-03 11:06:49	Weekly_config_only_backup_20220403020002-2022-04-03T02-00-05.tar	build 351	Local	287	Yes	No	No

FTD デバイスのバックアップ取得 ②

- ・ バックアップの取得対象とする FTD デバイスを指定

Backup Management Backup Profiles

Managed Device Backup

FTDv01

Managed Devices

Retrieve to Management Center

Start Backup

Storage Location: /var/sf/remote-backup

Note: Backup the Firepower 9300/ 4100 chassis configuration before initiating a backup of the logical Threat Defense devices configured on it.

- ① バックアップ取得対象の FTD デバイスを選択
- ② 取得したバックアップファイルを FMC へ移動する場合、Retrieve to Management Center にチェックを入れる。チェックを入れなければバックアップファイルは FTD デバイスの /var/sf/backup に保存される
- ③ Start Backup をクリック

FTD デバイスのバックアップ確認

- バックアップ処理がスタートしたことを Task Tab (system の左隣) で確認
- 完了後に Backup Management のページをスクロールダウン、Device Backups に取得したバックアップファイルの存在を確認

The screenshot displays the Cisco Firepower Management Center interface. The top navigation bar includes 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and a user profile 'admin'. The main content area is divided into 'Backup Management' and 'Backup Profiles'. Under 'Backup Management', there are buttons for 'Firepower Management Backup', 'Managed Device Backup', and 'Upload Backup'. A blue notification box states: 'Info New backups found on system. Importing backup information.' Below this is a table for 'Firepower Management Backups' with columns for System Information, Date Created, File Name, VDB Version, Location, Size (MB), Configurations, Events, and TID. The table lists two backup entries for 'Cisco Firepower Management Center for VMware v7.0.1.1'. A blue arrow points down to the 'Device Backups' section, which contains a table with columns for System Information, Date Created, File Name, VDB Version, Location, Size (MB), Configurations, Events, and TID. The table lists one backup entry for 'FTDv01 Cisco Firepower Threat Defense for VMware v7.0.1.1'. The 'Download', 'Delete', and 'Move' buttons for this entry are circled in red.

20+ total | 0 waiting | 1 running | 0 retrying | 20+ success | 0 failures

Backup

Backup: FTDv01_20220525154627
Checking the database

Backup Management Backup Profiles

Firepower Management Backup Managed Device Backup Upload Backup

Info
New backups found on system. Importing backup information.

Firepower Management Backups

<input type="checkbox"/>	System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
<input type="checkbox"/>	FMCv70 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-22 11:07:37	Weekly_config_only_backup_20220522020002-2022-05-22T02-00-05.tar	build 353	Local	457	Yes	No	No
<input type="checkbox"/>	FMCv70 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-15 11:07:35	Weekly_config_only_backup_20220515020001-2022-05-15T02-00-05.tar	build 353	Local	454	Yes	No	No

Device Backups

<input type="checkbox"/>	System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
<input type="checkbox"/>	FTDv01 Cisco Firepower Threat Defense for VMware v7.0.1.1	2022-05-25 15:55:20	FTDv01_20220525154627.tar	build 353	Local	121	Yes	No	No

Download Delete Move

- バックアップファイルは、管理用 PC ローカルにダウンロードして保存しておく (リストアで利用)

FMC のバックアップ取得 ①

- FMC 自身のバックアップを取得

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The main navigation bar includes 'System / Tools / Backup/Restore / Backup Management'. The 'Backup Management' section is active, showing a table of 'Firepower Management Backups'. A callout box on the right provides instructions for navigating to the Backup/Restore section.

① System (歯車マーク) → Backup/Restore を選択
② (FMC を新規でインストールした場合) デフォルトでスケジューリングされた FMC のバックアップデータが存在していれば、その一覧が表示されている
③ Firepower Management Backup をクリック

<input type="checkbox"/>	System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
<input type="checkbox"/>	FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-22 11:07:20	Weekly_config_only_backup_20220522020002-2022-05-22T02-00-05.tar	build 351	Local	451	Yes	No	No
<input type="checkbox"/>	FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-15 11:06:42	Weekly_config_only_backup_20220515020002-2022-05-15T02-00-05.tar	build 351	Local	318	Yes	No	No
<input type="checkbox"/>	FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-08 11:06:54	Weekly_config_only_backup_20220508020002-2022-05-08T02-00-05.tar	build 351	Local	317	Yes		
<input type="checkbox"/>	FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-01 11:07:01	Weekly_config_only_backup_20220501020002-2022-05-01T02-00-04.tar	build 351	Local	312	Yes		
<input type="checkbox"/>	FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-04-24 11:06:47	Weekly_config_only_backup_20220424020002-2022-04-24T02-00-05.tar	build 351	Local	312	Yes		
<input type="checkbox"/>	FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-04-17 11:06:58	Weekly_config_only_backup_20220417020002-2022-04-17T02-00-05.tar	build 351	Local	290	Yes		
<input type="checkbox"/>	FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-04-10 11:06:37	Weekly_config_only_backup_20220410020002-2022-04-10T02-00-04.tar	build 351	Local	281	Yes		
<input type="checkbox"/>	FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-04-03 11:06:49	Weekly_config_only_backup_20220403020002-2022-04-03T02-00-05.tar	build 351	Local	287	Yes	No	No

FMC のバックアップ取得 ②

- ・ バックアップ取得における各項目を設定

Backup Management Backup Profiles

Create Backup

Name

Storage Location /var/sf/backup/

Back Up Configuration

Back Up Events

Back Up Threat Intelligence Director

Email Not available. You must set up your mail relay host.

Copy when complete

Cancel Save As New Start Backup

- ① バックアップの名前を入力、ここでは“FMCv01-backup-20220525”とする
- ② FMC の設定のバックアップを含める場合にチェックを入れる (デフォルト On)
- ③ イベントログや、Threat Intelligence Director のデータをバックアップに含める場合にチェックを入れる (デフォルト Off)
- ④ バックアップ取得後にメール通知を行う場合に設定
- ⑤ バックアップ完了後に SCP サーバへバックアップファイルをコピーする場合にチェックを入れる (デフォルト Off)

FMC のバックアップ取得 ③

- バックアップファイルを SCP サーバへコピーする際に各項目を指定し、バックアップを開始

Backup Management Backup Profiles

Create Backup

Name

Storage Location

Back Up Configuration

Back Up Events

Back Up Threat Intelligence Director

Email Not available. You must set up your mail relay host.

Copy when complete

Host

Path

User

Password

SSH Public Key To use ssh keys place this public key in your authorized_keys file.

① SCP サーバの情報を入力
② Start Backup をクリック

参考: スケジューリングバックアップ

- FMC にて、FMC 自身および FTD デバイスのバックアップ取得を、スケジューリングで自動化することが可能

The screenshot displays the FMC configuration interface. At the top, there are navigation tabs: Policies, Devices, Objects, AMP, Intelligence, Deploy, and a search bar. Below these, there are sections for Logging, Monitoring, Health, and Tools. The Tools section is expanded, showing options like Backup/Restore, Scheduling, Import/Export, and Data Purge. A blue arrow labeled '1' points to the 'Scheduling' option. In the center, there is a calendar view for May 2022, with a blue arrow labeled '2' pointing to the 'Add Task' button. Below the calendar, there is a 'New Task' form. A blue arrow labeled '3' points to the 'Job Type' dropdown menu, which is set to 'Backup'. The form also shows 'Schedule task to run' set to 'Recurring', 'Start On' set to May 25, 2022, and 'Repeat Every' set to 1 week. The 'Run At' is set to 4:00 AM on Saturdays. The 'Job Name' is 'Weekly FTD device backup' and the 'Backup Type' is 'Device'.

① System (歯車マーク) → Schedulingを選択
② Add Task をクリック
③ スケジュールタスクとして Backup を選択し、FMC もしくは FTD デバイスのバックアップ取得スケジュールを作成

参考: FMC バックアップスケジューリングタスクの自動生成

- FMC を新規にインストールした場合には、FMC 自身のバックアップ取得をウィークリーで実施するように、タスクが自動的に作成される

Edit Task

Job Type

Schedule task to run Once Recurring

Start On

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Backup Type Management Center Device

Backup Profile

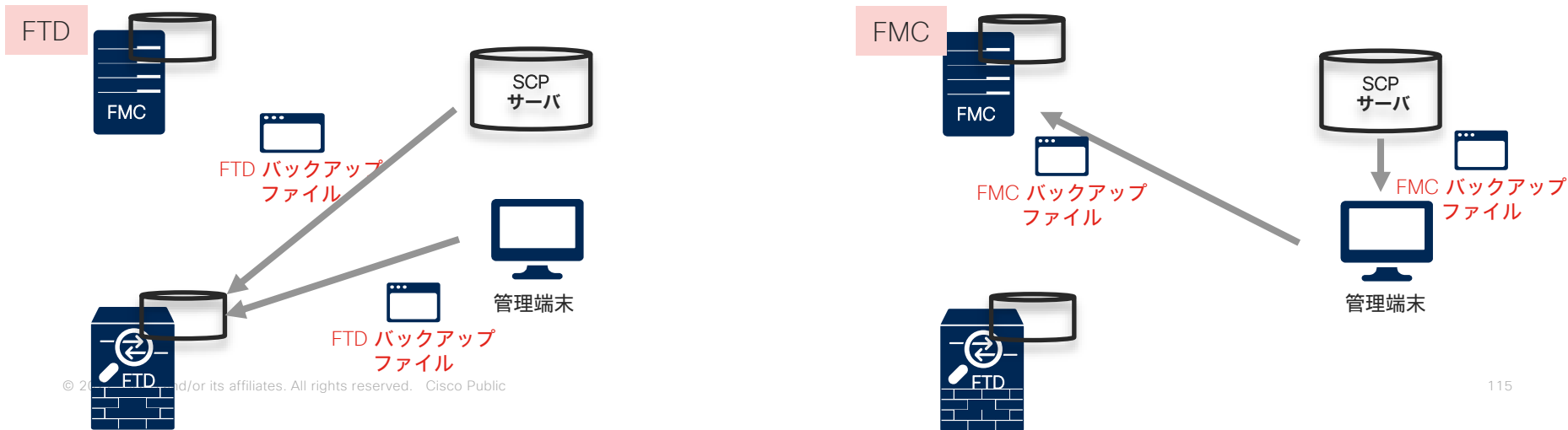
Comment

This was automatically set up during installation.

Email Status To [Not available. You must set up your mail relay host.](#)

リストアについて

- FTD リストアは、取得済みのバックアップファイルを SCP サーバ、もしくは FTD ローカルにアップロードして実施
- FMC リストアは、取得済みのバックアップファイルを FMC ローカルにアップロードして実施
- FMC, FTD とともにリストア時にはバックアップ取得時のソフトウェアはパッチレベルまで同一にしておく必要がある
- FTD リストア時にはさらに SRU, VDB も同一バージョンが必要 (FMC は不要)



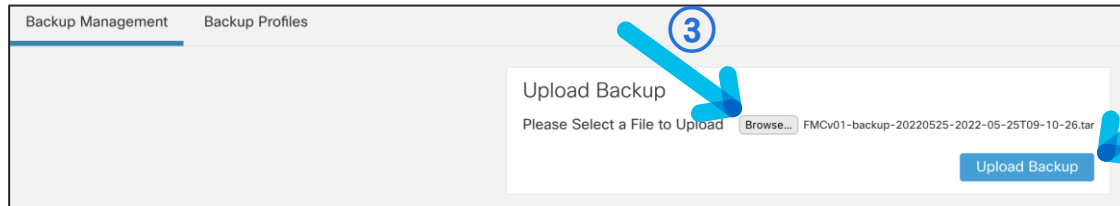
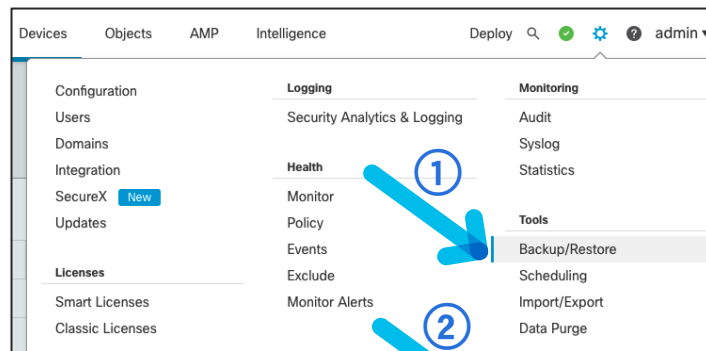
本章のリストアに関する操作の流れ

- FMC のバックアップファイルのアップロード
- FMC のリストア
- FTD デバイスのリストア (ローカルからのリストア)
- FTD デバイスのリストア (SCP サーバからのリストア)
 - SCP サーバは、管理ネットワークに存在している PC を利用
 - FTD, FMC とともに HA でもリストアは可能

FMC のバックアップファイルのアップロード ①

- ・ 機器交換等で、リストアに使用するバックアップファイルが FMC ローカルに存在しない場合には、取得済みの FMC バックアップファイルを、FMC ローカルにアップロード

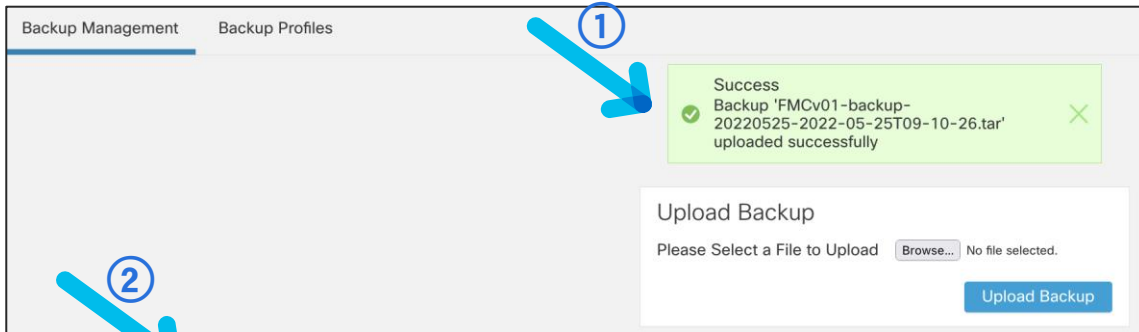
- ① System (歯車マーク) → Backup/Restore を選択
- ② Upload Backup をクリック
- ③ Browse をクリックし、管理 PC に準備済みの FMC バックアップを指定
- ④ Upload Backup をクリックし、アップロードを開始



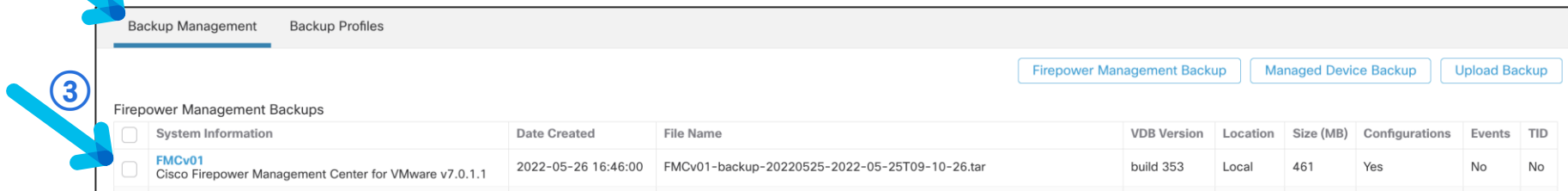
(注) リストア先の FMC は、バックアップを取得した FMC とソフトウェアバージョンとパッチを合わせて準備する。VDB や SRU はバックアップデータに含まれているバージョンで上書きされる

FMC のバックアップファイルのアップロード ②

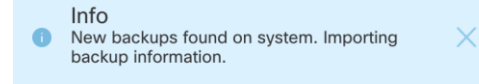
- ・ アップロードした FMC のバックアップファイルが認識されていることを確認



- ① アップロードが完了したメッセージを確認
- ② Backup Management をクリック (更新)
- ③ アップロードした FMC のバックアップファイルが認識されていることを確認



(注) アップロード直後に②を実施した場合、右のメッセージが表示され、ファイルが一覧に表示されないことがある。この場合は、まだFMCがファイルに含まれている情報を読み込んでいるため、数分待って再度②を実施すること



FMC のリストア ①

- ・ リストアに使用するバックアップファイルを選択し、リストアを実施

Backup Management Backup Profiles

Firepower Management Backup Managed Device Backup Upload Backup

Firepower Management Backups

<input type="checkbox"/>	System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
<input checked="" type="checkbox"/>	FMCv01 Cisco Firepower Management Center for VMware v7.0.1.1	2022-05-26 16:46:00	FMCv01-backup-20220525-2022-05-25T09-10-26.tar	build 353	Local	461	Yes	No	No

Restore Download Delete Move

- ① リストアに使用する FMC のバックアップファイルをチェック
- ② Firepower Management Backups のファイル一覧の下にある Restore をクリック
- ③ Replace Configuration Data をチェックし、Restore をクリックしてリストアを開始

Info
You are about to replace or modify key system files. The system will be rebooted at the end of the restore process.

Restore Backup

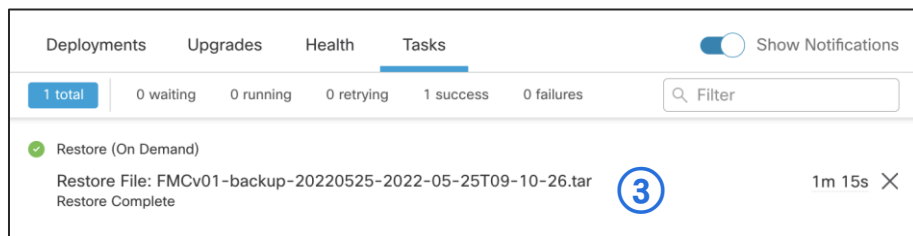
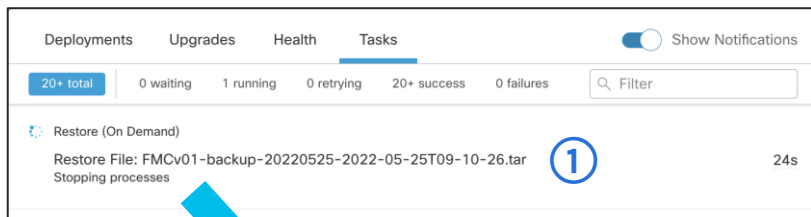
Backup Name FMCv01-backup-20220525-2022-05-25T09-10-26.tar

Replace Configuration Data

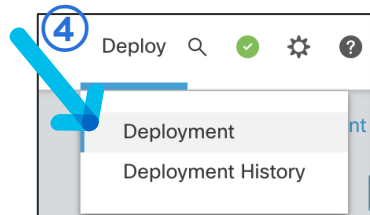
Cancel Restore

FMC のリストア ②

- ・ リストアの途中で FMC が自動的に再起動する。再起動後、FMC にログインし、リストアが無事に終わったことを Task Tab で確認、その後 FTD デバイスに deploy を実施



②



- ① リストア処理がスタートしたことを確認
- ② 自動的に再起動した FMC にログイン
- ③ Task Tab で FMC のリストアが無事に終わったことを確認
- ④ FTD デバイスに deploy を実施

FMC のリストア ③

- ・ もしも FTD デバイス up-to-date になっていた場合 (deploy が必要になっていない場合) は、Force Deploy の実施を推奨

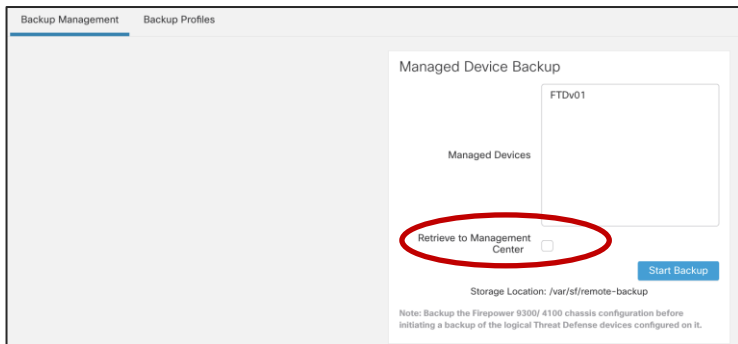
The screenshot illustrates the steps to perform a Force Deploy on a Cisco FTD device in FMC:

- ① Devices → Device Management にアクセス
- ② 対象 FTD デバイスの Edit (鉛筆マーク) をクリック
- ③ General タブの General カテゴリの Edit (鉛筆マーク) をクリック
- ④ Force Deploy の矢印をクリック
- ⑤ Deploy をクリックし、Force Deploy を実施

The deployment confirmation dialog shows: "You have selected 1 device to deploy" and "Deployment Notes: You can optionally add notes about the configuration changes".

FTD デバイスのリストア (ローカル) ①

- FTD のバックアップを取得する際に、Retrieve to Management Center にチェックをいれていなければ、FTD の /var/sf/backup/ にバックアップファイルが保存されている。この場合には、そのファイルを利用してリストアが可能



```
> expert
admin@FTDv70-1:~$ cd /var/sf/backup/
admin@FTDv70-1:/var/sf/backup$ ls -atl
total 122780
drwxr-xr-x  2 www  www    4096 May 26 08:35 .
-rw-r--r--  1 www  root 125716480 May 26 08:35 FTDv01_20220526173126.tar
drwxr-xr-x 77 root  root    4096 May 25 07:20 ..
```

FTD コンソールの expert モードでバックアップファイルの存在を確認可能

(注) リストア先の FTD は、バックアップを取得した FTD とソフトウェアバージョンとパッチ、および VDB や SRU を合わせて準備する必要あり

FTD デバイスのリストア (ローカル) ②

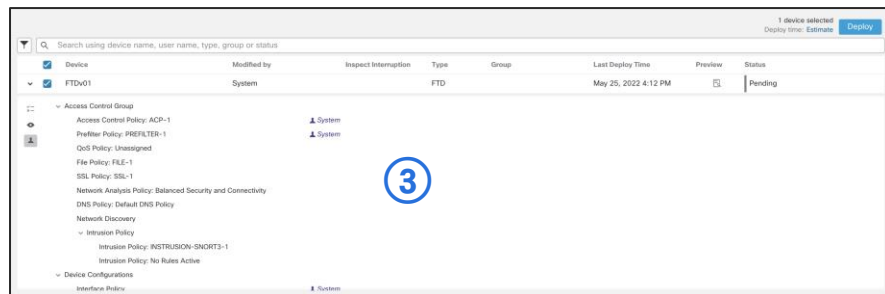
- FTD の CLISH (コンソール) でリストアコマンドを実行、バックアップファイルの詳細を確認

```
> restore remote-manager-backup FTDv01_20220526173126.ta ①  
  
Device model from backup :: Cisco Firepower Threat Defense for  
VMware  
This Device Model :: Cisco Firepower Threat Defense for VMware  
  
***** ② *****  
Backup Details  
*****  
Model = Cisco Firepower Threat Defense for VMware  
Software Version = 7.0.1.1  
Serial = 9AR5P6F3V0F  
Hostname = FTDv70-1  
Device Name = FTDv01  
IP Address = 10.71.153.76  
VDB Version = 353  
SRU Version =  
Manager IP(s) = 10.71.132.200  
Backup Date = 2022-05-26 17:31:26  
Backup Filename = FTDv01_20220526173126.tar  
*****
```

- ① restore コマンドを FTD の CLISH で実施
- ② バックアップファイルに含まれる情報を確認

FTD デバイスのリストア (ローカル) ③

- バックアップファイルの内容に問題がなければ、リストアを開始。FTD デバイスは自動的に再起動する。再起動後は FMC から deploy を実施、もしも FTD デバイスが up-to-date であれば、Force Deploy を推奨



***** Caution *****

Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches versions from backup manifest before proceeding.(Running 'show version' command on FTD, displays Model Name and version details).
Restore operation will overwrite all configurations on this device with configurations in backup.

If this restoration is being performed on an RMA device then ensure old device is removed from network or powered off completely prior to proceeding with backup restore.

Are you sure you want to continue (Y/N) y
Restoring device

②

- ① バックアップファイルの内容に問題がなければ y を入力してリストアを開始
- ② FTD へのリストアが実施され、FTD デバイスが自動的に再起動
- ③ FTD デバイスへの deploy を FMC から実施

(注) FTD デバイスへの Force Deploy 方法は FMC のリストア時と同じ

FTD デバイスのリストア (リモート SCP) ①

- FTD デバイス交換時等で FTD デバイスのローカルにバックアップファイルが無くても、SCP サーバに FTD デバイスのバックアップファイルがあれば、それを直接指定して CLISH (コンソール) でリストアコマンドの実行が可能、あとはローカルからのリストアと同じ

```
> restore remote-manager-backup location 10.71.132.191 cisco /home/ FTDv01_20220525154627.tar  
Enter SCP password:
```

```
Device model from backup :: Cisco Firepower Threat Defense for VMware  
This Device Model :: Cisco Firepower Threat Defense for VMware
```

```
*****
```

Backup Details

```
*****  
Model = Cisco Firepower Threat Defense for VMware  
Software Version = 7.0.1.1  
Serial = 9AR5P6F3V0F  
Hostname = FTDv70-1  
Device Name = FTDv01  
IP Address = 10.71.153.76  
VDB Version = 353  
SRU Version =  
Manager IP(s) = 10.71.132.200  
Backup Date = 2022-05-25 15:46:27  
Backup Filename = FTDV01_20220525154627.tar  
*****
```

- restore コマンドを FTD の CLISH で実施、引数に SCP サーバの IP アドレスやユーザ名、パス、ファイル名を指定
- SCP サーバにログインするパスワードを入力
- バックアップファイルに含まれる情報を確認

(注) リストア先の FTD は、バックアップを取得した FTD とソフトウェアバージョンとパッチ、および VDB や SRU を合わせて準備する必要あり

FTD デバイスのリストア (リモート SCP) ②

- バックアップファイルの内容に問題がなければ、リストアを開始。FTD デバイスは自動的に再起動する。再起動後は FMC から deploy を実施、もしも FTD デバイスが up-to-date であれば、Force Deploy を推奨

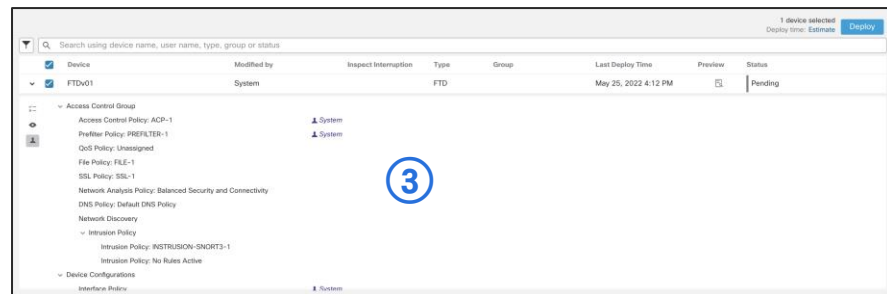
***** Caution *****

Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches versions from backup manifest before proceeding.(Running 'show version' command on FTD, displays Model Name and version details).
Restore operation will overwrite all configurations on this device with configurations in backup.

If this restoration is being performed on an RMA device then ensure old device is removed from network or powered off completely prior to proceeding with backup restore.

Are you sure you want to continue (Y/N) y
Restoring device

②



- ① バックアップファイルの内容に問題がなければ y を入力してリストアを開始
- ② FTD へのリストアが実施され、FTD デバイスが自動的に再起動
- ③ FTD デバイスへの deploy を FMC から実施

(注) FTD デバイスへの Force Deploy 方法は FMC のリストア時と同じ



The bridge to possible